IJARSCT

ISSN (Online) 2581-9429

Impact Factor: 6.252

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

Volume 2, Issue 7, May 2022

Ethereum Blockchain based Repository for Criminal Data Containment

Pinak Pandit[1], Rohit Sonar[2], Ashutosh Raykar[3], Suvas Wagh[4], Dr. M. A. Pradhan[5]

Student, Computer Department, AISSMS College of Engineering, Pune, India [1,2,3,4]

Faculty, Computer Department, AISSMS College of Engineering, Pune, India [5]

Abstract: *Crime in India is increasing at an alarming rate. However, the main issue is these activities are not clearly registered and are not stored effectively. Mostly in our Indian Management system Data is stored in the traditional Relational databases Systems which are prone to SQL injection attacks. . The main reason to maintain criminal records in a blockchain is that sensitive data like criminal records shouldn't be altered by anyone. There have been instances where criminal records have either been wiped or altered. It is not uncommon for corrupt officials to bribe in order to keep their criminal records clean and misuse their position. Consequently, police records can sometimes be altered or wiped out easily. A decentralized system on the blockchain platform for storing criminal records is the only way to prevent this. This ensures that no one can change or interfere with the records, and it eliminates the possibility of data being modified. The main motivation is to eliminate all the disadvantages of handling and storing criminal records in traditional database systems by incorporating the criminal data on a blockchain platform.*

Keywords: Blockchain, Information security, Ethereum, Decentralized Application Development, Web3.js

I. Introduction

A criminal record or RAP sheet is a summary of a person's criminal history. Even though criminal records differ from country to country, one thing remains the same which is that they are highly sensitive records which cannot be manipulated in any way by anyone unauthorized. When this information is stored in a traditional database, there is a possibility that it will be leaked, manipulated, or completely deleted by malicious users or threat actors. The blockchain has a role to play in this situation. Like a logbook, once data is added to the blockchain, it cannot be changed or removed. Data, once added to a blockchain, cannot be altered or deleted. In other terms blockchain is a system of recording information, which is immutable i.e., the information once stored cannot be altered or removed. One cannot hack into a blockchain as one can hack into the traditional databases using attacks such as SQL injections. As of right now, large quantities of data are stored in traditional databases, which means they are highly vulnerable to cyberattacks such as SQL injection attacks or unlawful data manipulation by corrupt officials. Along with the above issues in the traditional database, the databases can crash resulting in total loss of data. Hence incorporating the data into a blockchain is a solution to all the problems that still persist in the traditional database management systems.

II. RELATED WORK

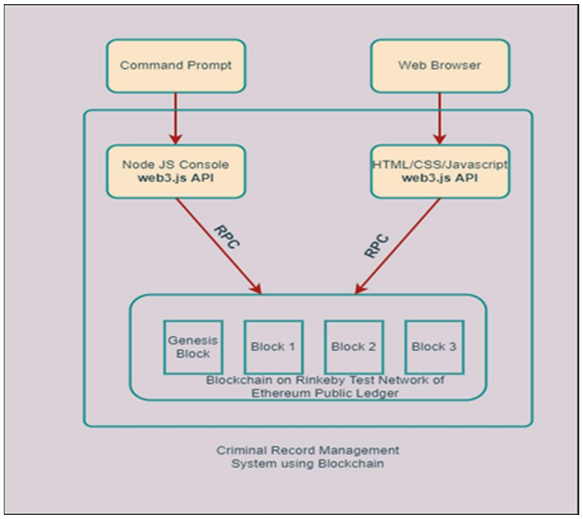
The data integration into the blockchain and to remove the disadvantages of the traditional databases is crucial. We have briefly discussed some of the existing research articles that are connected to our work in this part. The detailed survey of the papers which we have referred is given below:

[1] proposes that it would be possible to preserve criminal records' authenticity and rigidity using a blockchain, as well as securing data from adversaries. Data is deconcentrated and decentralized using P2P networks which further helps to prevent any illegal changes in the information. Also highlighted in their article was how incorporating criminal records into a blockchain will reduce the effects, also Integrating a thorough accountability procedure will significantly reduce the likelihood of tampering with criminal records information and will eliminate the possibility of corruption in law enforcement. Keeping the data safe and making the tedious task of managing the data easy, our system provides ways for the authorities to efficiently maintain criminal records. In [2], the authors propose implementing a blockchain-based

DOI: 10.48175/IJARSCT-4390

solution for handling both cognizable and non-cognizable offenses, creating a secure way for filing FIRs. In the proposed system, trust in the police is not required by the general public. The Four stakeholders participate in the system: the court, law enforcement admin, investigating officer, and the suspect. By implementing a decentralized solution, stakeholders will be able to keep track of all activities and protect the digital FIR from inadequacies. Officers will verify the details and adjust the complaint in the system depending on the complaint and evidence provided. They also maintain crime information in order to track the most wanted or top criminals in the country. Criminal Records Management System Online plays an important role in consummating the needs of all police officials by automating existing manual systems with the help of computerized equipment and full-fledged computer software in order to preserve valuable data/information for a longer period of time and make it easier for police officers to access the information. All records are saved digitally in this system. It gives improved prospects for the organization's progress in terms of quality and transparency. [3]. [4] shows that, despite the fact that the world is becoming more technically adept, systems still lack security. For enhanced data security, integrity, and reusability, Blockchain is being used to store criminal records. Concerned complaints are given a cryptographically generated hash key that may be used to check the integrity of the block. A blockchain is a piece of software that combines cryptographic algorithms, hash chains, and a consensus mechanism to enable online services like consensus, permanence, and provenance. [5] proposes utilizing blockchain technology to secure the FIR. The fundamental principles of distributed ledger technology are applied, and it is also the police department of India's future. The data in this technology is protected by a cryptographically constructed block. A few of the algorithms utilized include SHA-256 and a hash tree.

III. PROPOSED METHODOLOGY:-



We propose to build a Ethereum Blockchain based Repository for Criminal Data Containment, to function and maintain Confidentiality, Integrity and Availability of the data to be stored i.e., the Criminal Records. In addition to keeping the information secure, the blockchain technology will prevent the hackers from being able to hack the system or hack into a particular block, causing it to not impact the security of the other blocks. Because of its decentralized and distributed structure, blockchain is flexible and difficult to manipulate.

By enhancing the power of decentralization, SHA-256 will also increase the security of the system, Due to a unique hash derived from the previous block's hash and the block's transactions, every block is unique. In Hashing, the input value creates an entirely new ID after every change in values in the system, which helps us catch the criminals since we cannot reverse engineer the process.

In addition to the basic functionality of creating and accessing a criminal record, we will add functions such as registering FIR's, monitoring the criminal's behavior and health. Our application will serve as a repository of the court sentencing information for a particular criminal as well as notify the respective police officer if a criminal under their watch is summoned for a court hearing.

The main job that our application will get done is that the disadvantages of the traditional databases i.e., vulnerability to SQL injection and database crashing will overcome

DOI 10.48175/IJARSCT-4390

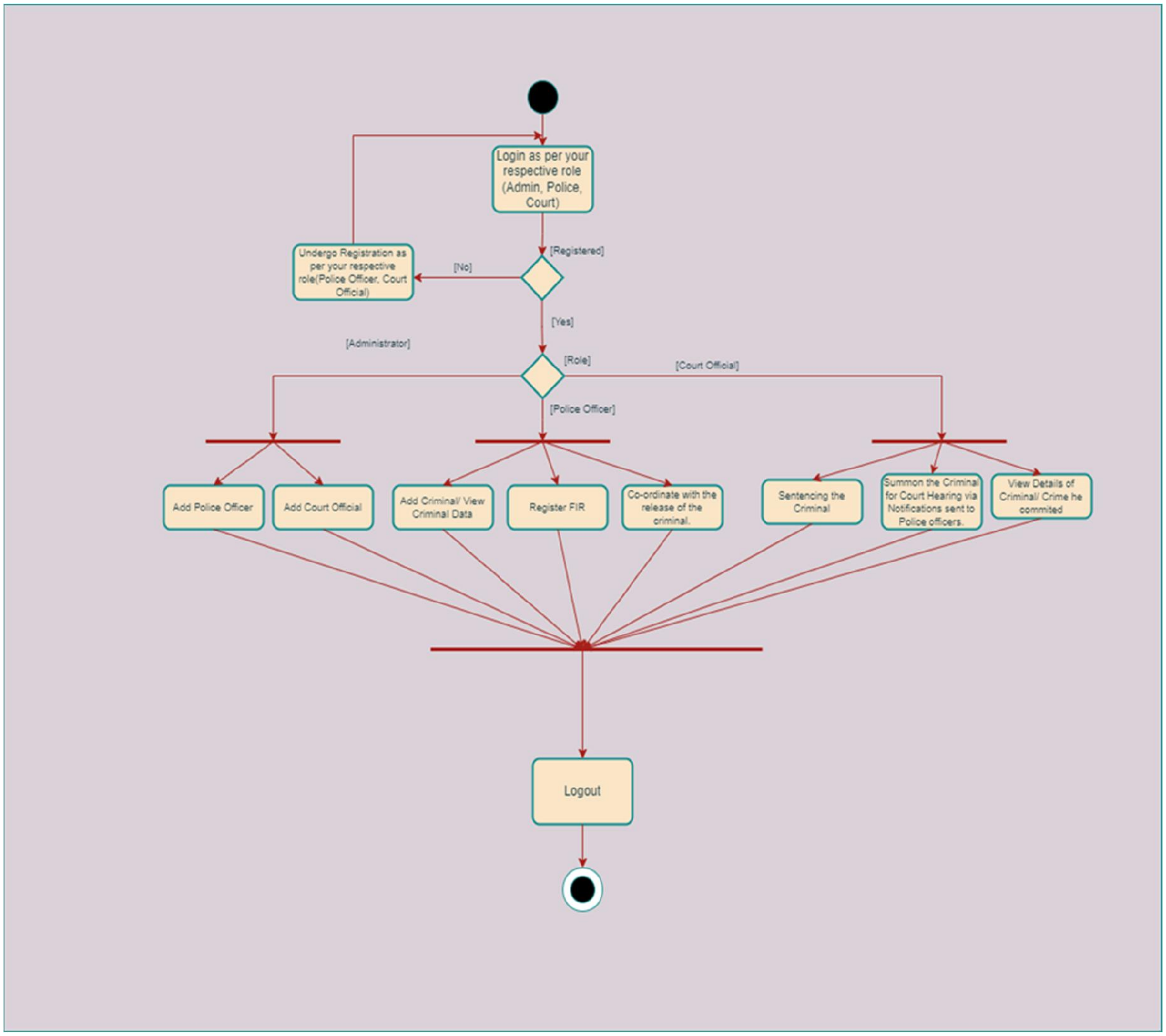
IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

Impact Factor: 6.252

Vol. X, Issue xx, <Month> 2022


Login as per your respective role (Admin, Police, Court)
[Registered]
[No]
Undergo Registration as per your respective role(Police Officer, Court Official)
[Yes]
[Administrator]
[Role]
[Court Official]
[Police Officer]
Add Police Officer
Add Court Official
Add Criminal/ View Criminal Data
Register FIR
Co-ordinate with the release of the criminal.
Sentencing the Criminal
Summon the Criminal for Court Hearing via Notifications sent to Police officers.
View Details of Criminal/ Crime he commited
Logout

IV. CRYPTOGRAPHY IN BLOCKCHAIN:

'Blockchain' is a peer-to-peer network; it is made up of two terms, 'block' and 'chain'. The data records in a block are called records, and the blocks stored in a chain are called a public database. As cryptography is used to link the lists, it is the most necessary and fundamental requirement for establishing a blockchain. In a blockchain thus the blocks are added to a growing list of records over time.

In a Blockchain, there are two types of Cryptographic algorithms

1. asymmetric-key algorithms
2. hash functions.

In order to provide participants with a single view of the blockchain, hash functions are used. In general, blockchains use the SHA-256 hashing algorithm. [7]

SHA-256 ALGORITHM

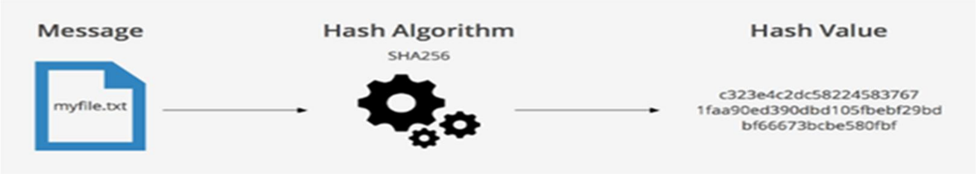
With a digest length of 256 bits, the Secure Hash Algorithm (Secure Hash Algorithm, FIPS 182-2) is a good cryptographic hash function. Security Hash Algorithm (SHA) was developed by NIST, followed by SHA-256 (the SHA-2 family), where 256 represents the hash length in bits. SHA-256 is similar to SHA-1. Like SHA-1, SHA-256's message is padded & divided into 512-bit blocks. [8].

- As a result of cryptographic hash functions, the blockchain provides the following benefits:
- An avalanche effect occurs when a small change in data causes a significant change in the outcome.

DOI 10.48175/IJARSCT-4390

- A unique output results from each input.
- If any input is passed through the hash function, it will always produce the same output.
- Speed - In a short period of time, the output can be generated.

Reverse engineering is impossible since we cannot generate the input from the output and hash function.



A blockchain is commonly defined as a "distributed ledger with smart contracts". [9,10].

- Ledgers are important because they record all changes to the business objects they record. Collaboration between organizations involves maintaining a consistent copy of a replicated ledger by collaborating with one another.
- Smart contracts define how new transactions can be added to a ledger and how queries may be made against it. The lifecycle of a business object can be described in code in smart contracts. The lifecycle explains how the object is created, updated, and queried. [9].
- Blockchain ledgers are unique in two ways:
- Distributed: Each actor in a blockchain network holds an identical copy of the ledger. Blockchain ledgers are decentralized since no single actor owns them. In a process called consensus, all replicated copies are kept synchronized with each other.
- Immutable: Every block of transactions in a blockchain ledger is cryptographically hashed and linked to the previous block, so tampering with them is impossible. The hashes of any transaction in this chain cannot be changed without invalidating the chain.
- All the Blockchain Structures fall into three categories:
- Architecture of Blockchain systems with a public architecture is open to everyone, so anyone can participate and access the system (e.g., Ethereum, Bitcoin).
- Private Blockchain Architecture: The private system differs from public blockchain architecture in that it is only controlled by members of a specific organization, or by users who have been invited to join.

Consortium Blockchain Architecture: This blockchain structure can be used by several organizations. A consortium's preliminary users establish and control procedural guidelines.

V. EXPECTED RESULTS

Criminal records will be stored in the blockchain by the developed software. Additionally, the data will be uploaded to Inter Planetary File System (IPFS), a reliable distributed system for storing and retrieving files. The data will not be manipulated in any way and the CIA Triad will apply, i.e., Confidentiality, Integrity, and Availability.

Each Criminal will have a unique SHA 256 Hash which will identify him uniquely and all the data that is known and stored of that particular criminal can be traced easily in our IPFS. Along with the storage of Criminal Data, users can further file FIR's, the court can summon a particular criminal via notifications sent through email.

VI. CONCLUSION

Due to the growing amount of records, an effective system of record keeping and information exchange has become more important in today's globalized society. Criminal records are one of the most sensitive documents, and their security is paramount. This is where blockchain technology adds value. No one can manage the peer-to-peer network thanks to the blockchain ledger, which decreases the danger of data manipulation and makes data deletion impossible.

The Distributed Crime Record Management System will be more safe and secure in storing such sensitive information, giving it an advantage over traditional databases and handwritten records.

REFERENCES

[1] "CRAB: Blockchain Based Criminal Record Management System" by Maisha Afrida Tasnim, Abdullah Al Omar, Mohammad Shahriar Rahman, Md. Zakirul Alam Bhuiyan, SpaCCS 2018 Conference Paper: Springer Nature

DOI 10.48175/IJARSCT-4390

Switzerland AG 2018.

[2] “Police Complaint Management System using Blockchain Technology” by Ishwarlal Hingorani, Rushabh Khara, Deepika Pomendkar, Nataasha Raul, Proceedings of the Third International Conference on Intelligent Sustainable Systems [ICISS 2020].

[3] “Online Criminal Record Management System” by Pratibha Mishra, Ghousiya Bee. N, Mohsina S, Mubashshira Sultana, Surbhi Singh, IJESC Volume 9 Issue No. 05 2019.

[4] “Blockchain Based Crime Record Management System” by Bhushan Dube, Mahesh Gangarde, Ankit Singh, Jitendra Pawar, Sagar Dhanake. JAC: A Journal Of Composition Theory. ISSN: 0731-6755.

[5]“A Method to Secure FIR System using Blockchain” by Antra Gupta, Deepa V. Jose. International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8, Issue-1, May 2019.

[6] Blockchain Definition: What You Need to Know. (n.d.). Retrieved May 25, 2022, from https://www.investopedia.com/terms/b/blockchain.asp

[7] Cryptography in Blockchain Explained | by Amarpreet Singh | Brandlitic | Medium. (n.d.). Retrieved May 25, 2022, from https://medium.com/brandlitic/cryptography-in-blockchain-explained-df11fe1bd0f7

[8] What Is SHA-256 Algorithm: How it Works and Applications [2022 Edition] | Simplilearn. (n.d.). Retrieved May 25, 2022, from https://www.simplilearn.com/tutorials/cyber-security-tutorial/sha-256-algorithm

[9] Smart Contracts and Chaincode — hyperledger-fabricdocs main documentation. (n.d.). Retrieved May 25, 2022, from https://hyperledger-fabric.readthedocs.io/en/release-2.2/smartcontract/smartcontract.html

[10] Nakamoto, S. (n.d.). Bitcoin: A Peer-to-Peer Electronic Cash System. www.bitcoin.org

DOI 10.48175/IJARSCT-4390