International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Immutable Block Chain Criminal Data Repository

S.Sivakrishna[1], Renukachowdary[2], P.G.V.Vamsi[3], V.Manjusha[4], P.P.Sahitya[5], Y.S.Nagarjuna[6]

[1]Assistant Professor, Cse Department, Vsm College Of Engineering, Ramachandrapuram, Dr.B.R.Ambhedkar Konaseema Dt, Andhra Pradesh - 533255
[2,3,4,5,6] Student, Cse Department, Vsm College Of Engineering, Ramachandrapuram, Dr.B.R.Ambhedkar Konaseema Dt, Andhra Pradesh - 533255

Abstract:
As cities and towns grow and become more urbanized, the graph of crime rates is becoming more.Blockchain can take the role of those voluminous criminal records by creating a network where papers are safe and secure, freely accessible, and impenetrable. Blockchain is a peer-to-peer (P2P) network that facilitates data decentralization. In order to guarantee data security and integrity, this system will be built on the immutability feature of blockchain. By facilitating greater objectivity and consistency and making it easier for third parties to monitor tamper-evident transactions, this blockchain-based process can lower the risk factors for corruption and improve the transparency and accountability of criminal records. Law enforcement will also be more successful if legitimate criminal records are promptly accessed by the appropriate administrativeauthorities.

Keywords: decentralization, blockchain, security, criminal records, and authentication

Introduction

Criminal histories are important information to have during an interrogation and the identification of crimes. The legal system in our nation has been addressing the deeper security of criminal records for many years, making them easily accessible and maintaining their integrity. Using and managing these data can be difficult, even for highly-level governments. The fact that distinct state law enforcement agencies maintain different databases makes it difficult for different government departments to interchange data. One major obstacle is when certain states fail to transmit the numbers at all or send them much later than the volume was made available. Furthermore, protracted delays in the release of crime data have hindered policymakers' ability to act appropriately within the necessary timeframe. The likelihood of unauthorized alteration is steadily increasing due to the increased expense of maintaining security.

One of the three cornerstones of any government is justice. A system for storing information has the ability to enhance the current system and fulfill all the needs for a judicial system that operates well. In this piece, we examined the viability of managing citizens' criminal histories through the use of a blockchain-based system. Blockchain technology has the potential to be used to address these issues. A blockchain was first created as a chain of blocks with an expanding list of records, or blocks, connected

by cryptography. Every block is made up of its own cryptographic hash, which serves as its own identification. Time stamps and data that needs to be preserved are also included. It is an immutable, shared ledger that makes data recording easier and lowers the possibility of data manipulation. [2] The blockchain's three primary components that guarantee efficiency, security, and trust are as follows:

Distributed ledger technology: The distributed ledger and its original transaction data were accessible to all network users. Because this public ledger only keeps track of a single transaction, it eliminates the repetitive tasks that are usual in traditional business networks.

Immutable records: Once a transaction is entered into the shared ledger, it cannot be altered or modified by any other member. When there are mistakes in the transaction log, a new transaction is added to fix the problem, making two transactions appear.

Smart contracts: These are self-executing agreements with the specifications of a peer- to-peer contract. Intelligent contracts are essentially blockchain-based programs that activate when certain conditions are met. They are typically employed to automate the agreement's implementation, which eliminates the need for middlemen and saves time by allowing all parties to view the outcomes right now.

It can also initiate the subsequent action to automate the workflow when the necessary criteria are met.

Numerous cyber-attacks could jeopardize a central database, with the majority having a major impact on the data's integrity and dependability. The most frequent and highly destructive attack types on the system that have been launched recently are SQL injection and DDoS attacks. Specifically, distributed denial of service attacks (DDoS) overwhelm systems, servers, and networks with traffic, utilizing up bandwidth and resources. Procedures are unable to comply with valid requests and can occasionally lead to data loss and irreversible hardware problems.

The goal of SQL injection is to expose the data within the database.[3] Since blockchain technology is immutable, its decentralized feature guarantees that data integrity is not impacted by intrinsic issues like software and hardware malfunctions. Blockchain data is stored in several copies on every network node, making any changes visible to the network as a whole. Since several nodes validate updates from a single node, fake data cannot enter the blockchain. For a single block to be affected by a destabilization attempt, at least 51% of the nodes on that blockchain must be simultaneously attacked. An exponential decrease in the likelihood of such attacks occurs with an increase of nodes. One of the primary goals of our system is to avoid evidence tampering in court by keeping the original records and transaction log on the blockchain and storing the data in the cloud.

METHODOLOGY

Our goal in writing this paper was to propose the notion of creating a more intricate and safe system that keeps track of all criminal records. We will talk about and walk through our system's architecture in this part. Using a technique that connects each block to form a chain, our proposal employs a distributed, decentralized network to store criminal data.

In order to comprehend the procedure, let's assume there are four stages:

a. **The Reporting Officer**: The reporting officer gets the details of the offense that was committed. After that, the officer records the information, which causes a block to be generated and the paperwork to be eliminated.

b. **Data validation:** Upon block creation on the network, a copy of the block is distributed to each peer on the network for confirmation and validation. The block won't be confirmed by the other network

members if it has been altered throughout the procedure within one of the peer networks. As a result, the network would only contain the confirmed data.

c. **Data availability throughout the peer network:** After the data has been verified by the miners, it is saved permanently on each blockchain node.

Verified data is kept in an immutable format, which allows authorized users to access it with ease from any location.4.Access Data: Those who have successfully authenticated themselves can access data that has a distinct case id and hash associated with it. Any type of data can be stored in a block. All of the criminal records will be stored in this block of our system. When validated, its unique value—a hash—serves as a fingerprint that can be seen by every other node in the network..

- Every block has the following information:
- the block hash
- an encrypted hash of the block that came before it
- the Merkle tree root hash algorithms
- measuring the amount of time that has passed since 1970-01-01 at 00:00 UTC
- the goal of the present problem
- The nonce

It also includes the previous block's hash number, creating a chain of information- containing blocks. As soon as new information becomes available, it is added to a new block. Data is linked chronologically when blocks are chained together when they are full.

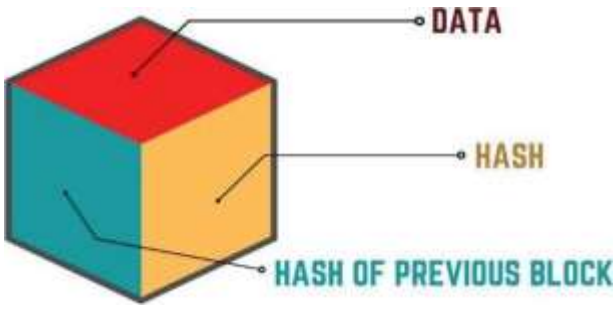

Figure1.A BLOCK

A. Hashing

A mathematical operation known as a hash can convert any length of input into an encrypted output of a fixed length. Hence, its one-of-a- kind hash value remains constant in size, regardless of the initial data or file size. The original data cannot be recovered by decrypting hashing because it is a one-way cryptographic operation. The mathematical algorithm known as SHA-256 (secure hashing algorithm-256) forms the basis of our proposed method.

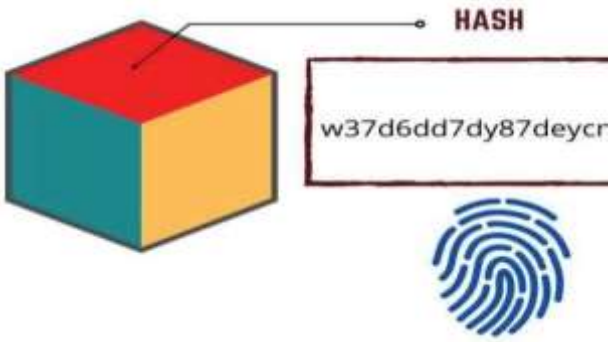

Figure 2. Hash inside a Block

One of the most widely used encryption and authentication protocols is SHA-256. Furthermore, it offers safe hashing of passwords.

SHA256 is secure because:

- it is difficult to recover the original data from the hash value.
- Two messages with the same value are not likely to occur.
- The hash value is changed by a minute change in the original data.

The previous block's hashA chain known as a blockchain is created by the hash of the previous block. Without it, the network would just consist of individual blocks laid out on top of each other, with no sense of order or connection between them. Each new block includes the hash of the one before it. Similarly, a lengthy chain is created by each block including a hash of the one before it.

1) The Genesis Block: The first block from which the blockchain is created is known as the Genesis Block. It is frequently referred to as block zero since it serves as the foundation for adding additional blocks to create a shape of a sequence of blocks. In the blockchain, a credential to the previous block is stored in every block. The Genesis block does not have a preceding block to which it can be referenced. It is technically possible to process data up to the Genesis block without processing any data at all since the last hash value is set to 0. Every subsequent block, starting with the first, would have its hash set to the hash of the most current block. After each new block is added to the blockchain, the process is repeated to generate its unique hash.

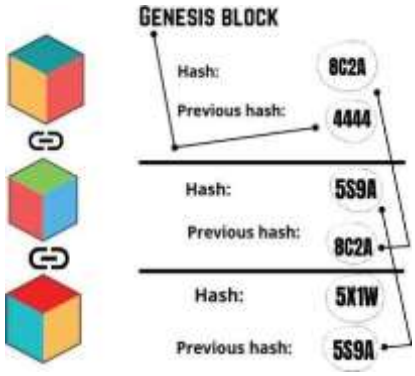

Figure 3. The blockchain's structure

B. How does a Blockchain Merkel Tree Operate?

One of the most essential components of blockchain technology is a Merkle tree. All of the transactions are combined into one block in this mathematical data structure, which is made up of hashes from

different data blocks. Ensuring consistency and verifying the accuracy of data is facilitated by the effective and secure verification of content. The Merkle tree, for instance, can be used to determine the status of a certain criminal record. The complete blockchain does not need to be downloaded; instead, we just need to request vertical evidence and a particular tree branch in order to access the data.

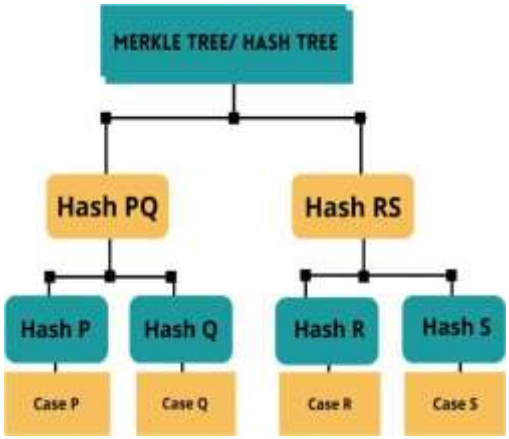

Figure 4. Merkel Tree Structure

C. Dates and Times

Each block has a distinct serial number called a timestamp, which is used by the blockchain network to identify when a block was mined and verified.

D. The Present Difficulty Goal Complexity gauges how time-consuming it is to determine a block's hash value. Greater complexity necessitates more processing. Because more power is needed to generate the same amount of blocks than usual, the network is more resistant to cyber attacks. In summary, a network is safer the more complex it is.

E. Workproofing

For the proof-of-work consensus method to produce new blocks on the blockchain network, difficult computational puzzles must be solved. To put it simply, this procedure is known as "mining," In the network, the nodes engaged in mining are referred to as "miners." Economic rewards are used as incentives for mining transactions, and rival miners will get a little transaction fee in return.

E.Nonce

In order to tweak the nonce value, miners use a 32-bit randomly generated whole number. A nonce can only be utilized once. For instance, a miner must discover the nonce value before adding a block with a criminal record to the blockchain.

EXISTING MODEL

The current system for managing criminal records faces numerous challenges in terms of accessibility, security, and integrity. Traditional methods of record-keeping often involve centralized databases that are vulnerable to tampering, corruption, and unauthorized access. These systems are not only susceptible to data breaches but also lack the transparency and accountability necessary for efficient law enforcement. Manual record updates and maintenance procedures are time-consuming, and the risk of errors or intentional manipulation exists. Additionally, the lack of a standardized and secure platform for sharing criminal records among administrative authorities hinders the timely and effective exchange of information crucial for law enforcement agencies. The existing system falls short in adapting to the

evolving landscape of urbanization and technological advancements, necessitating a more robust and secure solution for criminal record management.

PROPOSED MODEL

The proposed "Blockchain-Based Criminal Record Database Management" system offers a transformative solution to overcome the limitations of the existing criminal record management systems. The proposed system seeks to transform the storage, access, and sharing of criminal records by harnessing the power of blockchain technology.

The key innovation lies in the use of a decentralized, tamper-proof blockchain network. This ensures the immutability of criminal records, eliminating the risk of unauthorized tampering and enhancing data integrity. Each record, once added to the blockchain, becomes a permanent and unchangeable part of the ledger, providing a transparent and auditable history of all transactions.

The peer-to-peer nature of the blockchain facilitates decentralization, reducing the dependency on a single central authority. This not only enhances security but also ensures the system's resilience against potential attacks or system failures. The use of cryptographic techniques further strengthens the security measures, making it highly resistant to unauthorized access.

The proposed system addresses the lack of transparency and accountability in the existing system by enabling a transparent and traceable audit trail of all record modifications. This not only instills confidence in the accuracy of the information but also allows for accountability in case of any discrepancies.

ACTIVITIES

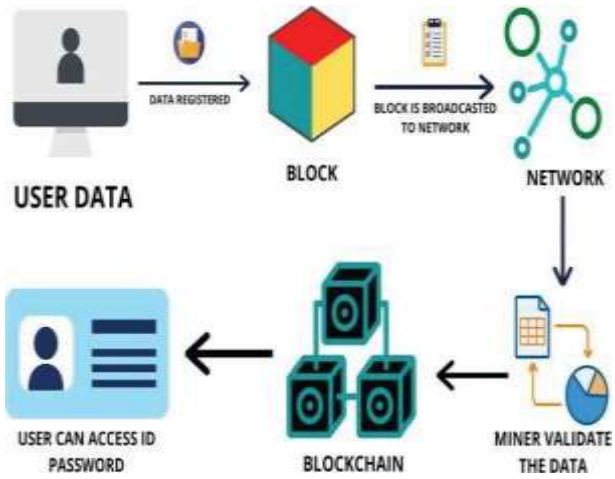

Fig. 5. How the System Operates

This part will demonstrate how our project operates.Digitallysigned, encrypted, and network-stored criminal records are first produced on a decentralized network.

The user initiates operation by notifying the appropriate authorities of the crime that has occurred. The reporting officer then compiles all of the network's information about the crime. After then, a block is created using the data that has been gathered. The created block contains the details of the crime, such as its hash value and smart contacts for potential authentication in the future.

The blockchain network will disseminate the aforementioned block. Every peer in the network is informed about the newly created block.To determine the nonce value of a given block, miners on the

network compete with one another. The nonce is a value that the miners modify in order to validate the block.

When a miner finds the nonce value and at least half of the network's miners agree with it, the block is validated. Here, validation means that the data has not been influenced by any other peer group.

The data is saved on the blockchain when it has been verified. Those who have verified their identity can access the blockchain's data by using a special case ID and password. The state police departments, high courts, district courts, federal and state governments, and the supreme court are examples of verified peer-to-peer network users in this context. Therefore, adding to the blockchain network was restricted to a responsible individual or official inside the nation's legal system.

HISTORY

Fowzi and associates; [4] The goal of their endeavor is to create a digital file storage system. For easy access to the data, an application is made available to all authorities. Because it offers a variety of functions (such as registering crimes, updating evidence, and accessing case reports), this program is simple to use. Our productivity will rise and we will save time using this program. Thus, this guarantees the jurisdictional system's transparency.

In Maisha et al.'s study [5], a system that illustrates how criminal records are digitally preserved was presented. This system stores the data in an encrypted format on a local database, managed by the designated administrator.The integrity of criminal records will be preserved by this system, which will prevent any unauthorized user from making any modifications.

Hassija, Vikas, and others; [6] They offered suggestions on how to get around the issues with local server file storage with a blockchain-based approach. Their work exemplifies the use of mathematical representation in a consortium blockchain paradigm to generate a legitimate block. Additionally, they clarified how smart contacts work for verification reasons.

A system has been suggested by Muhammad Baqer et al. [7] wherein the home ministry of the country will function as a central server. Every police station will take an active part in the server. The records are maintained by the designated police officer. The ministry representatives will next review and double-check the information. This system is known as "Third Eye." In any event, if data is altered, the relevant authorities may become aware of it. Data security is therefore guaranteed.

Those associated with Kirti: [8] An encrypted local server is their proposed method for storing the data. This helps with effective e- governance by ensuring the data is secure and intact.

REVIEW OF LITERATURE

A blockchain system based on the idea of one blockchain, one criminal case was presented by Vaishnavi et al. [9]. However, in the long run, this method makes the entire criminal record blockchains lengthy and difficult to operate in a country with a high case rate of density population. On the other hand, our proposed system consolidates various criminal records into a single blockchain, which makes it easier and more compact to execute operations. Transparent blockchain technology was investigated by Bhushan et al. [10] as a potential tool for keeping tabs on police complaints. Public blockchains give the system greater transparency. However,Consensus protocols are more resource-intensive and environmentally unfriendly, which makes them difficult to implement in applications because they would be expensive. Cost savings compared to the public blockchain are a result of the consortium blockchain's lower resource consumption. Note that it is not inexpensive, though. It might be worthwhile

to invest to observe the difference, as you are essentially altering the system. But in the long run, you'll save more money and get more benefits.In their work, A. T. Dini et al.
[11] presented a decentralized blockchain-based system for storing criminal records of citizens. The main goal of our study is used to eliminate the need for paperwork and facilitate easy data access for any necessary authority. This will allow the legal system to access the blockchain at any time for legal purposes. It improves the coherence of the entire judicial system.

APPLICATION

This article primarily aims to review the literature on blockchain technology as an adjunct to existing cybersecurity applications, both public and private. Our main objective is to present a community-driven approach to investigate cybersecurity and blockchain more thoroughly by looking at how the two topics connect. In order to do this, we will critically assess recent research and works on blockchain cybersecurity and apply the lessons we learn to create fresh approaches.

FUTURE AREA

Global adoption of blockchain technology is expected to be quite positive. Its prospective application is mostly in the field of online safety. The data is safe and verified even though the blockchain ledger is distributed and open to the public. Cryptography is used in encryption to close security gaps like illegal data modification. Government organizations could benefit greatly from the concept of blockchain as it could aid in the management of massive amounts of data. When blockchain is implemented, it will become an effective data management system that might raise these institutions' productivity and efficiency. Moreover, since data on centralized servers is vulnerable to hacking, data loss, and human error, cloud storage will be more durable and secured against hacking thanks to blockchain's decentralized security feature. [12] Blockchain technology has enormous potential in the healthcare industry in the future. One of the main industries in India lacking adequate data is healthcare. assembling different information
takes a lot of time to learn about the patients. It ought to put more of an emphasis on helping people who most need health services. Thus, with the aid of IoT and wearables, it may use blockchain in this situation to store and update important medical data in real-time, such as blood pressure and sugar level. Additionally, it assists physicians in keeping a close eye on high-risk patients around-the-clock and informing and warning family members and caregivers of any emergencies. [13]

FINAL MENTION

Since local databases can be altered to store data, we suggested an unchangeable blockchain-based system using a decentralized network to keep track of illegal activity. In order to address this problem, we divided the data among other organizations while preserving data transparency and updated our data using digital signatures. Thanks to the network's accessibility, we may be able to collect statistical data that improves internal processes, justice proceedings, and the legal system. With
the rightimplementation, blockchain, a new technology, can give better control over criminal records. Technology, in and of itself, is powerless to effect change; nevertheless, when combined with innovative ideas, technology can produce a successful product that advances society.

RECOGNITION

We are grateful to Dr. Akhilesh Das Gupta, a student of Ms. Shagun Saboo**'s at the Institute of Technology and Management in New Delhi, India, for his guidance. We greatly improved our manuscript with her insightful comments.

REFERENCES

1. "Using blockchain technology to enhance public sector data anagement2017;McKinsey&Company.https:/
2. /www.mckinsey.com/business}functions/mcki nsey-digital/our-insights/improving-data- management-in-the-public-sector-using- blockchain.
3. "IBM Blockchain: An Overview of Blockchain Technology," ibm.com. What is blockchain?, https://www.ibm.com/in-en/topics.
4. "Common Cyberthreats - Cyber Attacks?" Cisco.
5. The types of cyberattacks are described in https://www.cisco.com/c/en_in/products/securi ty/commoncyberattacks.html#~. [4] F. J. BARROW, "A Look at the Criminal Record Management System from Somalia's Perspective," www.grin.com, 2019.
6. 491032, https://www.grin.com/document. In 2018, Maisha A. Tasnim and colleagues published "CRAB: Blockchain Based Criminal Record Management System" in SpaCCS, LNCS 11342, pages 294–303. 10.1007/978-3-030-05345-1_25 is the doi.
7. Police FIR Registration and Tracking Using Consortium Blockchain, Hassija V., Patel A., Chamola V. (2021). Within the book Advances in Machine Learning and Computational Intelligence, edited by Patnaik S., Yang XS., and Sethi I. Intelligent Systems Algorithms. Singaporean Springer.
8. The article 10.1007/978-981-15-5243-4_75
9. IEEE/OSA/IAPR, "Proposed E-Police System for Enhancement of E-Govemment Services of Bangladesh," Muhammad Baqer Mollah et al., 2012.
10. 10.1109/ICIEV.2012.6317444 is the DOI.
11. "E-FIR using E-Governance," Kirti Marmat et al., IJIRST, vol. 3, 2016. JIRSTV3I2024.pdf,
12. available at http://www.ijirst.org/articles. [9] "A Transparent Blockchain for Tracking Police Complaints," R. Pise, V. Swami, M. Hajgude, S. Godse, and K. Thombare, International Journal of Recent Technology and Engineering, vol. 9, no. 1, May 2020, pp. 973–976.
13. A2099059120.pdf can be found at https://www.ijrte.org/wp~content/uploads/pape rs/v9i1/.
14. M. Bhushan, C. Sagar, M. Ankit, and M. Jitendra, "AUTHOR NAMES FOR BLOCKCHAIN BASE CRIME RECORD MANAGEMENT SYSTEMS," July 2020.
15. [Online]. http://www.jctjournal.com/gallery/11-july-
16. 2020.pdf is accessible.
17. "Analysis of implementing blockchain technology to the Argentinian criminal records information system," by A. T. Dini, E. Gabriel Abete, M. Colombo, J. Guevara, B. S. Menchón Hoffmann, and M. Claudia Abeledo, IEEE Xplore, Nov. 01, 2018. 8584365
18. (https://ieeexplore.ieee.org/document) (retrieved June 19, 2021). [13] "Blockchain for Cybersecurity: A Comprehensive Survey," P. Bansal, R. Panchal, S. Bassi, and A. Kumar, IEEE Xplore,Apr. 01, 2020. 9115738
19. (https://ieeexplore.ieee.org).
20. The article "Blockchain for IoT-Based Healthcare: Background, Consensus, Platforms, and Use

Cases" was published in the IEEE Systems Journal in 2020. It can be accessed at doi: 10.1109/JSYST.2020.2963840. [14] P. P.
21. Ray, D. Dash, K. Salah, and N. Kumar.