Blockchain-Based Criminal Record Database Management

Aastha Jain
Information Technology and Engineering Department
Dr. Akhilesh Das Gupta Institute of Technology and Management
New Delhi, India
jainaastha0606@gmail.com

Soumyajit Das
Electronics and Communication Engineering Department
Dr. Akhilesh Das Gupta Institute of Technology and Management
New Delhi, India
soumyadas349@gmail.com

Anand Singh Kushwah
Electronics and Communication Engineering Department
Dr. Akhilesh Das Gupta Institute of Technology and Management
New Delhi, India
Email: anandrajput0787@gmail.com

Tushar Rajora
Computer Science and Engineering Department
Dr. Akhilesh Das Gupta Institute of Technology and Management
New Delhi, India
Email: tusharrajora72@gmail.com

Shagun Saboo**
Electronics and Communication Engineering Department
Dr. Akhilesh Das Gupta Institute of Technology and Management
New Delhi, India
Email: shagun.saboo98@gmail.com

2021 Asian Conference on Innovation in Technology (ASIANCON) | 978-1-7281-8402-9/21/$31.00 ©2021 IEEE | DOI: 10.1109/ASIANCON51346.2021.9544655

***Abstract*—With rapid urbanization and the advancement of cities and towns, the graph of crime rates is increasing gradually. Blockchain can replace those piled up criminal records with a network where documents are easily accessible and could not be tampered with, making them safe and Secure. Blockchain is a P2P (peer-to-peer network) that helps in the decentralization of data. This system will be based upon the immutability characteristic of blockchain to ensure the integrity and security of data. This blockchain-based process can reduce corruption risk factors by making it easier for third parties to monitor tamper-evident transactions and enabling greater objectivity and consistency, thus enhancing criminal record transparency and accountability. Furthermore, timely access of authentic criminal records to respective administrative authorities will make law enforcement effective.**

Keywords—Blockchain, security, criminal records, authentication, decentralization

I. INTRODUCTION

Criminal records play a crucial role in the interrogation and detection of crime. For many years, our country's judicial system has been dealing with securing those criminal records more profoundly in which accessibility becomes easy and security becomes intact. Even for high-level governments, managing and using these data can be a burden. Different state law enforcement agencies have separate databases, which hinders data exchange between various government agencies. A stumbling block is encountered when some states do not bother sending the numbers or sending them long after the volume was released. In addition, long delays in the publication of crime statistics have prevented policymakers from taking appropriate action in the required time. The existence of such multiple databases also increases the cost of its security, so the possibility of illegal modification is gradually growing. [1]

Justice is one of the three pillars of any government. In this regard, an information storage system will potentially improve the existing system and meet all the requirements for an efficient judicial system. In this article, we analyzed the possibility of implementing a blockchain-based system to manage citizen's criminal records. Blockchain technology can come into force to solve these problems. A Blockchain is originally a chain of blocks with a growing list of records, called blocks, linked together by cryptography. Each block consists of the cryptographic hash that is the unique identity of that particular block. It also includes timestamps and data to be stored. It is a shared and immutable ledger that facilitates recording data and reducing the risk of data tampering. [2]

Three main key elements in the blockchain that ensure trust, security, and efficiency are:

- **Distributed ledger technology:** All network participants could access the distributed ledger and its unaltered transaction records. This public ledger records only one transaction, removing the identical duplication of standard work in traditional corporate networks.
- **Immutable records:** After the transaction gets recorded on the shared ledger, no member could change or modify the transaction. If the transaction log contains errors, a new transaction gets added to correct the error, and two transactions appear.
- **Smart contracts**: These are self-executing contracts that contain the terms and conditions of a peer-to-peer agreement. Smart contracts are just programs stored on the blockchain, which runs when predefined needs get fulfilled. Usually, they are used to automate the execution of the agreement so that everyone involved can see the results immediately, without the need for intermediaries and wasting time. When the conditions are satisfied, it can also automate the workflow by triggering the following action.

A central database may be put in danger by many types of cyber-attacks, most of which would seriously affect the integrity and reliability of the data. SQL injection and DDoS attacks are the most common type of attack launched recently on the system which is highly destructive attacks. DDoS attacks, in particular, flood the systems, servers, and networks

978-1-7281-8402-9/21/$31.00 ©2021 IEEE

with traffic that drains resources and bandwidth. Procedures are incompetent to fulfill the required legitimate requests and sometimes result in permanent hardware issues and data loss. In SQL injection, it tries to reveal the information in the database.[3] The decentralized property of the blockchain ensures that inherent problems such as hardware and software errors do not affect data integrity due to the immutable nature of blockchain. Data in blockchain has multiple copies stored on each node of the network, due to which all changes are visible on the entire network. Multiple nodes verify data updated from a single node, and thus falsified data could not get into the blockchain. Any attempt to destabilize the system must involve simultaneous attacks on at least 51% of the nodes on a given blockchain to affect a single block. As the number of nodes increases, the probability of such attacks decreases exponentially.

One of the primary goals of our system is to ensure that evidence information is not tampered with during court trials by storing the data in the cloud and keeping the transaction log and original records in the blockchain.

II. Methodology

In this paper, we aimed to project an idea to develop a more profound and secure system that stores all the criminal records. In this section, we will discuss and demonstrate the architecture of our system. Our project is based on a decentralized and distributed network to store criminal data in a technique that connects all blocks to form a chain.

To understand the process, let us suppose we have four stages:

- **The Reporting Officer**: The reporting officer receives the information regarding the crime that took place. The officer then records the data, which results in generating a block, thus removing the paperwork.
- **Validation of data:** As soon as the block has been created on the network, a copy of that block is sent to all the network peers for verification/validation. During the process, if the block has been tampered with within one of the peer networks, it will not be verified by the rest of the network members. Hence only the verified data would be there on the network.
- **Availability of data across the peer network:** When the miners have validated the data, it permanently gets stored on every blockchain node. Data stored in the immutable form of data gets verified, and authenticated people can easily access the data from anywhere.
- **Access Data:** We can access the data with a unique case id and a hash associated with it by the authenticated people.

A block can store any information. In our system, this block will hold all the criminal records. It has a unique value called hash that acts like a fingerprint accessible across all the network peers once verified. Each block contains:

- the hash of the block
- a cryptographic hash of the previous block
- the root hash of the Merkle tree
- the time in seconds since 1970–01–01 T00: 00 UTC
- the goal of the current difficulty
- the nonce

It also contains the hash number of the previous block to make a chain of blocks containing information. As new data comes in, it enters into a new block. Once the block gets piled up with data, it is chained onto the previous block, making the data chained together in chronological order.

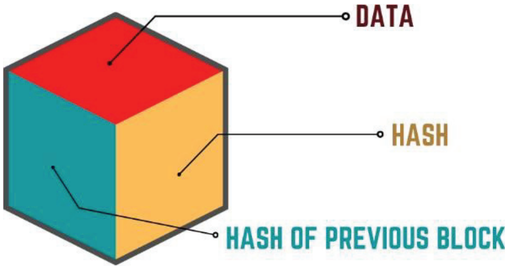

Fig. 1. A Block

A. Hash

Hash is a mathematical function that can convert an input of any arbitrary length into an encrypted output of a fixed length. Therefore, regardless of the original data or file size, its unique hash value is always the same size. On the other hand, hashing is a one-way cryptographic function that cannot be decrypted to retrieve the original data. We have proposed a system based on a mathematical algorithm called SHA- 256 (secure hashing algorithm -256).

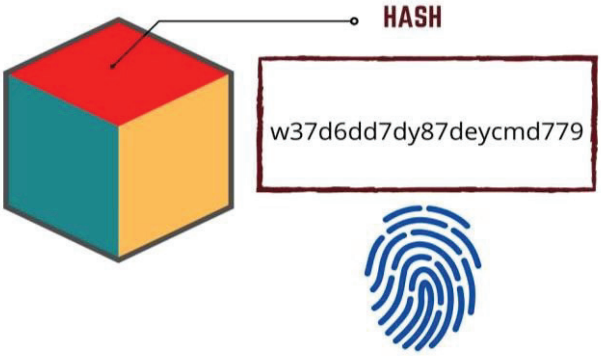

Fig. 2. Hash in a Block

1) SHA-256: It is one of the most popular authentication and encryption protocols. In addition to that, it provides secure password hashing.

Things that make SHA256 secure:

- It is challenging to restore the initial data from thehash value.
- It is unlikely to have two messages with the samevalue.
- A-minute change in original data alters the hashvalue.

B. Hash of the previous block

The hash of the previous block is what results in forming a chain termed a blockchain. Without this major component, there would be no interconnection and chronology between the blocks, and every block would be independently lying on the network. New Block contains the hash of the previous block. Similarly, every block has a hash of the previous one that forms a long chain.

1) *Genesis Block:* The Genesis Block is the first block from where the blockchain starts. It is the basis on which different blocks are added to a form of a series of blocks; as a result, it is often referred to as block zero. Every block stores a credential to the previous block in the blockchain. In the case of the Genesis block, there is no preceding block for reference. Technically, in the Genesis block, its last hash value is set to 0, meaning no data was processed before the Genesis block. The rest of the blocks have sequential numbers starting with one, and they would have the previous hash set to the hash of the last block. This combination is used to create its unique hash and this process repeats itself until all new blocks have been added to the blockchain.

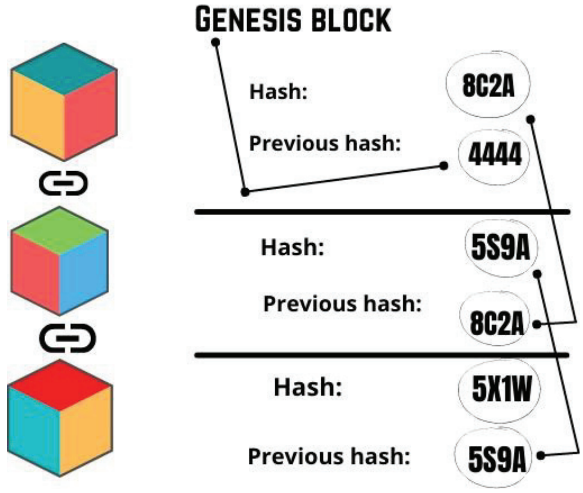

Fig. 3. Structure of a blockchain

C. How does a Merkel Tree work in a Blockchain?

A Merkle tree is one of the most fundamental parts of blockchain technology. It is a mathematical data structure consisting of hashes of different data blocks that summarize all transactions in one block. The efficient and safe checking of the content helps to ensure consistency and check the information of the data. For example, the Merkle tree will be effective in knowing the status of one particular criminal record. There is no need to download the entire blockchain; we need to ask for vertical proof and a specific branch of a tree to access the data.

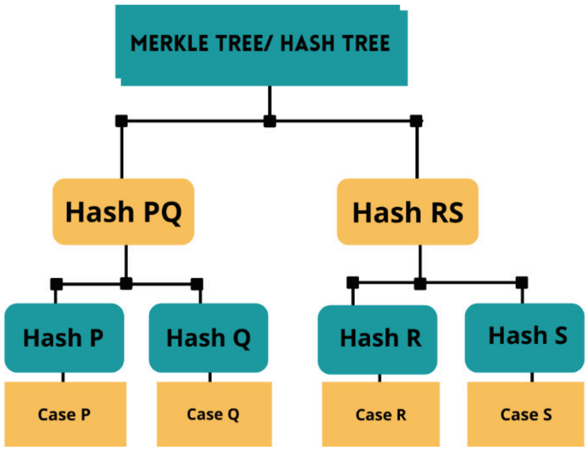

Fig. 4. Structure of a Merkel Tree

D. Timestamps

Every block contains a unique serial termed timestamps whose function is to mark the instance in which a block has been mined and validated by the blockchain network.

E. The current Goal of Difficulty

Complexity measures how tedious it is to find the hash value of a block. High complexity means that more computing power than usual is required to obtain the same number of blocks, making the network more secure against cyber-attacks. In short, the higher the difficulty, the safer the network.

F. Proof of Work

The proof-of-work consensus algorithm involves solving complex computational problems to generate new blocks on the blockchain network. In layman's terms, this process is called "mining," The nodes participating in mining in the network are called "miners." The incentive for mining transactions is an economic reward, and competing miners will receive a small transaction fee.

G. Nonce

A 32-bit generated random whole number that the miners adjust is known as nonce value. A nonce can is used only once. For example, a block having a criminal record is added to the blockchain only after a miner finds the nonce value.

III. Implementation

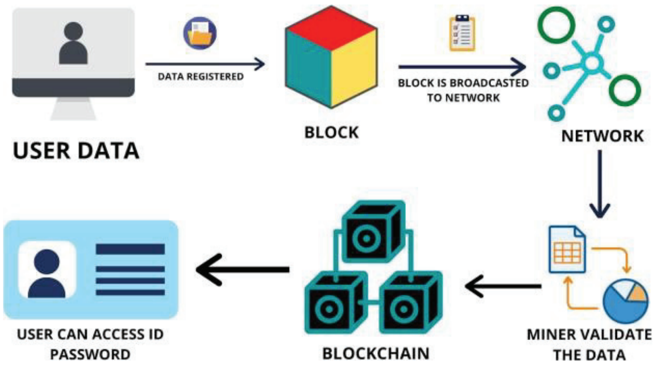

Fig. 5. Working of The System

In this section, we will see the working of our project. First, a decentralized network is created where Criminal records are digitally signed, encrypted, and stored on the network.

The functioning starts with the user reporting the crime that has taken place to the legitimate authority. The reporting officer then accumulates all the data regarding the crime on the network. Then, a block gets generated from the collected information. The block formed contains the information regarding the crime, its own, i.e., the hash value and smart contacts for authentication purposes in the future.

The above block will be broadcasted on the blockchain network. All the peers of the network get alerted about the block that has been created. Miners present on the network compete with one another in finding out the nonce value of that particular block. The nonce is value adjusted by the miners used for validation of the block. Once a miner finds out the nonce value, and if 51% of miners present on that network agree with that value, the block is validated. Validation here defines that no other peer group has tempered the data.

Once the data is validated, it is then stored on the blockchain. Authenticated people can assess the data from the blockchain with a unique case id and associated password. Here authenticated peer-to-peer network users are the supreme court, high courts, district courts, central and state governments, and different state police departments. Therefore, only a responsible person or authority in the country's judicial system could add to the blockchain network.

Similarly, if some more information is added for the same case, it can be added using the same methodology under the same case id. Also, if the case goes for the court trial, the judgment could be added further under case id by the court. Later we can filter the case id mentioned in smart contact to view all the blocks of a particular case.

IV. Background

Fowzi et al.; [4] Their project aims to develop a system that stores all the files digitally. An application is made available to all the authorities to get easy access to the data. This application is easy to use as it provides various operations (like registering the crime, updating evidence, searching reports of a particular case). This application will save our time and will increase productivity. Hence this ensures the transparency of the jurisdictional system.

Maisha et al.; [5] this paper presented a system that displays how criminal records are stored digitally This system records the information on a local database in the encrypted form by the assigned administrator This system will restrict all the illegitimate changes done by any unauthenticated user thus maintaining the integrity of criminal records.

Vikas Hassija et al.; [6] They suggested how a blockchain-based system can overcome the complications that occurred during file storage on local servers. Using a consortium blockchain-based model, they exhibit how mathematical representation can generate a valid block. They also explained how smart contacts work for verification purposes.

Muhammad Baqer et al.; [7] Have introduced a system in which the country’s home ministry will act as a central server. All the police stations will be active participants of the server. The assigned police official manages the records. After this, the ministry officials will overlook and cross-verify the data. They have named this system “Third Eye”. In any case, if data gets tampered it could come into the knowledge of the concerned authorities. Hence data security is ensured.

Kirti et al.: [8] They have proposed a system that holds the information in the encrypted form on an established local server this ensures the data is secured untampered and hence helps in effective e governance.

V. Literature Review

Vaishnavi et al.;[9] proposed a blockchain system that consists of the ideology of one blockchain having one criminal case. However, this method, in the long run, in a densely populated country where the cases are much higher, makes the entire blockchains of the criminal record a lengthy one and much challenging to operate while in our proposed system, we are generating a single blockchain that contains multiple criminal records making it compact and efficient to carry out an operation.

Bhushan et al.; [10] in their paper, discussed the use of transparent blockchain for tracking police complaints. Public blockchains offer more transparency to the system. Still, consensus protocols consume more resources and are not eco-friendly in any way, hence making the system to put in an application much more challenging as it would become costly. The consortium blockchain system is less expensive than the public because it uses fewer resources. However, point to be noted; it is not cheap. Since you are completely changing the system, it would make investments to see the change. However, in the long run, it will benefit you more and save the cost.

A. T. Dini et al.;[11] in their paper proposed a system to store citizen criminal records in a decentralized way by using blockchain technology. The key objective of our research paper is to remove the paperwork process involved and make the data get accessed easily by any authority required. Here, the judicial system will be able to gain access to the blockchain whenever needed. It makes the whole judicial system work much more coherently.

VI. Application

This paper focuses on the existing literature on blockchain as a supporting technology for cybersecurity applications, including privacy-related business areas. Our overarching goal is to provide a community-driven plan to better explore blockchain and cybersecurity by examining the interaction between the two frequently discussed areas. Toward this goal, we will critically examine current works and studies on blockchain cybersecurity and use our insights to develop new directions.

VII. Future Scope

Blockchain technology has a bright future ahead worldwide. Its future scope majorly lies in the field of Cybersecurity. Although the blockchain ledger is public and distributed, the data is secure and verified. Encryption gets done using cryptography to eliminate loopholes such as unauthorized data manipulation. The concept of blockchain could further help manage large amounts of data, which would be very useful for government agencies. The implementation of blockchain will make it an efficient data management system that could improve the performance and efficiency of these institutions. Also, the decentralized security feature of blockchain will make cloud storage more protected and robust against hacking as the data on a centralized server is exposed to hacking, loss of data, or human error. [12]

The future scope of blockchain technology in healthcare also is immense. Healthcare is one of the major sectors in India which have insufficient data. Compiling various details about the patients consumes a lot of time. Instead, it should focus on providing health services to those who need them most**.** Therefore, it could use blockchain here to store and update valuable patient data such as blood pressure and sugar level in real-time with the help of IoT and wearables. It also helps the doctors to monitor patients 24*7 who are prone to high risk and to inform & alert their caretakers & relatives in case of any emergency. [13]

VIII. CONCLUSION

Storing data in Local databases can be manipulated; therefore, we proposed an immutable blockchain-based system to maintain a criminal record on a decentralized network. To solve this issue, we have modified our data with digital signature and distributed the data among different entities to maintain data transparency. Easy availability of the information on the network could potentially lead us to generate statistical information which will improve the juridical system, justice actions, and internal processes. Blockchain is an emerging technology and can effectively create more robust control over criminal records if implemented carefully. Technology is just a raw material that alone cannot bring change, but technology processed with creative ideas renders a flourished product for the advancement of society.

ACKNOWLEDGMENT

We thank Ms. Shagun Saboo** student, Dr. Akhilesh Das Gupta Institute of Technology and Management, New Delhi, India for guiding us. Her valuable feedback remarkably enhanced our manuscript.

REFERENCES

[1] "Using blockchain to improve data management in the public sector," McKinsey & Company, 2017. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/using-blockchain-to-improve-data-management-in-the-public-sector.

[2] "What is Blockchain Technology? - IBM Blockchain," www.ibm.com. https://www.ibm.com/in-en/topics/what-is-blockchain.

[3] "Cyber Attack - What Are Common Cyberthreats?," Cisco. https://www.cisco.com/c/en_in/products/security/common-cyberattacks.html#~types-of-cyber-attacks.

[4] F. J. BARROW, "Criminal Record Management System In the Perspective of Somalia," www.grin.com, 2019. https://www.grin.com/document/491032.

[5] Maisha A. Tasnim et al., "CRAB: Blockchain Based Criminal Record Management System", SpaCCS, LNCS 11342, pp. 294–303, 2018. DOI:10.1007/978-3-030-05345-1_25.

[6] Hassija V., Patel A., Chamola V. (2021) Police FIR Registration and Tracking Using Consortium Blockchain. In: Patnaik S., Yang XS., Sethi I. (eds) Advances in Machine Learning and Computational Intelligence. Algorithms for Intelligent Systems. Springer, Singapore. https://doi.org/10.1007/978-981-15-5243-4_75

[7] Muhammad Baqer Mollah et al., "Proposed E-Police System for Enhancement of E-Govemment Services of Bangladesh", IEEE/OSA/IAPR, 2012. DOI:10.1109/ICIEV.2012.6317444.

[8] Kirti Marmat et al., "E-FIR using E-Governance", IJIRST, vol. 3, 2016. http://www.ijirst.org/articles/IJIRSTV3I2024.pdf.

[9] R. Pise, V. Swami, M. Hajgude, S. Godse, and K. Thombare, "A Transparent Blockchain for Tracking Police Complaints," International Journal of Recent Technology and Engineering, vol. 9, no. 1, pp. 973–976, May 2020. https://www.ijrte.org/wp-content/uploads/papers/v9i1/A2099059120.pdf .

[10] M. Bhushan, M. Ankit, M. Jitendra, and D. Sagar, "BLOCKCHAIN BASE CRIME RECORD MANAGEMENT SYSTEM AUTHOR NAMES," Jul. 2020. [Online]. Available: http://www.jctjournal.com/gallery/11-july-2020.pdf.

[11] A. T. Dini, E. Gabriel Abete, M. Colombo, J. Guevara, B. S. Menchón Hoffmann, and M. Claudia Abeledo, "Analysis of implementing blockchain technology to the argentinian criminal records information system," IEEE Xplore, Nov. 01, 2018.

[12] https://ieeexplore.ieee.org/document/8584365 (accessed Jun. 19, 2021).

[13] P. Bansal, R. Panchal, S. Bassi, and A. Kumar, "Blockchain for Cybersecurity: A Comprehensive Survey," IEEE Xplore, Apr. 01, 2020. https://ieeexplore.ieee.org/document/9115738.

[14] P. P. Ray, D. Dash, K. Salah, and N. Kumar, "Blockchain for IoT-Based Healthcare: Background, Consensus, Platforms, and Use Cases," IEEE Systems Journal, vol. 15, no. 1, pp. 1–10, 2020, DOI: 10.1109/JSYST.2020.2963840 .