IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 4, April 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 4, April 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1104013 |

Block Chain Based Criminal Record Management System

Kirti Singh, Saniya Singh, Omkar Gawde, Sumit Parmar

Third Year - Diploma in Information Technology, Thakur Polytechnic, Mumbai, India

Third Year - Diploma in Information Technology, Thakur Polytechnic, Mumbai, India

Third Year - Diploma in Information Technology, Thakur Polytechnic, Mumbai, India

Senior Lecturer, Dept. of Information Technology, Thakur Polytechnic, Mumbai, India

ABSTRACT *:* Criminal records are highly sensitive public records. By incorporating criminal records in a blockchain, authenticity and rigidity of records can be maintained; which also helps to keep the data safe from adversaries. Criminal record management systems play a critical role in maintaining public safety and administering justice. However, traditional systems face various challenges, including data tampering, privacy violations, and centralized control. This study proposes a blockchain-based criminal record management system that provides secure and immutable storage of criminal records, ensures data privacy and integrity, and promotes decentralized control.

The proposed system leverages blockchain technology to establish a distributed ledger that records all criminal records in a transparent and immutable manner. The system employs smart contracts to automate the management of criminal records, enabling efficient and reliable access to the information. Additionally, the system uses encryption techniques to ensure the confidentiality of sensitive information and protect it from unauthorized access

KEYWORDS – Blockchain technology, criminal records management, data privacy, access control, Immutable

I. INDRODUCTION

A blockchain-based criminal record management system is a revolutionary approach to managing criminal records. This system utilizes the blockchain technology, which is a decentralized and immutable ledger that records transactions in a secure and transparent manner. By using blockchain, a criminal record management system can ensure the accuracy and integrity of criminal records while providing increased security and privacy for individuals.

Traditionally, criminal records have been stored in centralized databases managed by government agencies or law enforcement organizations. These systems are often vulnerable to hacking, tampering, and errors, which can lead to inaccurate records and wrongful convictions. Furthermore, centralized systems can be accessed by unauthorized personnel, compromising the privacy and security of individuals. With a blockchain-based criminal record management system, individuals can have greater control over their own records and can grant or deny access to authorized parties. Additionally, the system can be designed to comply with data protection regulations and provide greater privacy for individuals.

A chief function of the government is to preserve data about individuals. Administering and utilizing these data can prove to be cumbersome, even for advanced governments. Different government law enforcement agencies have separate databases, which creates a barrier in the fluidity of data flow between different government agencies.

II. RELATED WORK

Various data sharing systems using blockchain have been developed Research work has been done on cloud data provenance architecture. Two such platforms are Prove Chain and Smart Provenance Prove Chain is decentralized cloud data provenance architecture that uses blockchain technology. When a user accesses data from the cloud, records are kept in the blockchain as transactions. It ensures that the

records cannot be tampered. In Prove Chain, the provenance auditor endorses provenance data by fetching transactions from the blockchain network by using blockchain-receipt which contains data in block and transactional information Here the Provenance Auditor (PA) cannot be fully trusted. Since PA has access to both user and provenance data; it can cause devastating damage to the system. To avoid this, the data is encrypted before uploading to the cloud. As such, the

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 4, April 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1104013 |

PA cannot directly access the data without the decryption key The Smart Provenance system is built on the existing Ethereum system, which uses smart contracts. These are used to store metadata of a file and include an event log. The event log is an immutable record consisting of the changes made to the file or data. This system can only guarantee honest behaviour if at least half of the users able to access the data and provenance are honest. There also must exist a secure platform for exchanging external keys among the users, so a user can provide access to other users

III. PROPOSED METHODOLOGY AND DISCUSSION

Step 1 - Design the system architecture: Based on the requirements of the government, a system architecture should be designed. The architecture should incorporate blockchain technology, which is decentralized, transparent, and secure. The system should also have a user-friendly interface to facilitate easy access to the records.

Step 2 - Choose the blockchain platform: The next step is to choose the appropriate blockchain platform for the system. There are several blockchain platforms available, such as Ethereum, Hyperledger Fabric, and Corda. Each platform has its own strengths and weaknesses, and the selection should be based on the specific needs of the system.

Step 3 - Integrate the system with existing infrastructure: The system should be integrated with the existing infrastructure of the agencies to ensure that the data can be accessed and shared seamlessly.

Step 4 - Test and deploy the system: The final step is to test the system thoroughly and deploy it. The system should be tested for its performance, scalability, and security. Once the system is deployed, it should be monitored regularly to ensure that it is functioning as expected.

IV. PROPOSED ALGORITHM

1. User Verification: The system should first verify the identity of the user who is accessing the system. This could be done using a combination of username, password, and two-factor authentication.
2. Record Creation: When a new criminal record needs to be added to the system, the authorized user will create a new record. The record will contain details such as the name of the offender, the crime committed, and the date and location of the offense.
3. Hashing and Encryption: Once the record has been created, it will be hashed and encrypted to ensure that the data is secure and cannot be tampered with.
4. Validation: The record will then be validated by a network of nodes on the blockchain. This validation ensures that the data is accurate and that there are no duplicates or errors in the record.
5. Adding to Blockchain: Once the record has been validated, it will be added to the blockchain. This creates a permanent and tamper-proof record of the criminal offense that can be accessed by authorized users at any time. Access Control: The system should have access control mechanisms in place to ensure that only authorized users can access the criminal records. This helps to prevent unauthorized access and tampering of the records.
6. Search and Retrieval: Authorized users can search and retrieve criminal records from the blockchain- based system based on different criteria, such as the name of the offender, the date of the offense, and the type of crime committed.
7. Updating Records: In the event of new information regarding a criminal record, authorized users can update the record on the blockchain. However, this update will also go through the same validation process to ensure the accuracy of the new data.

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

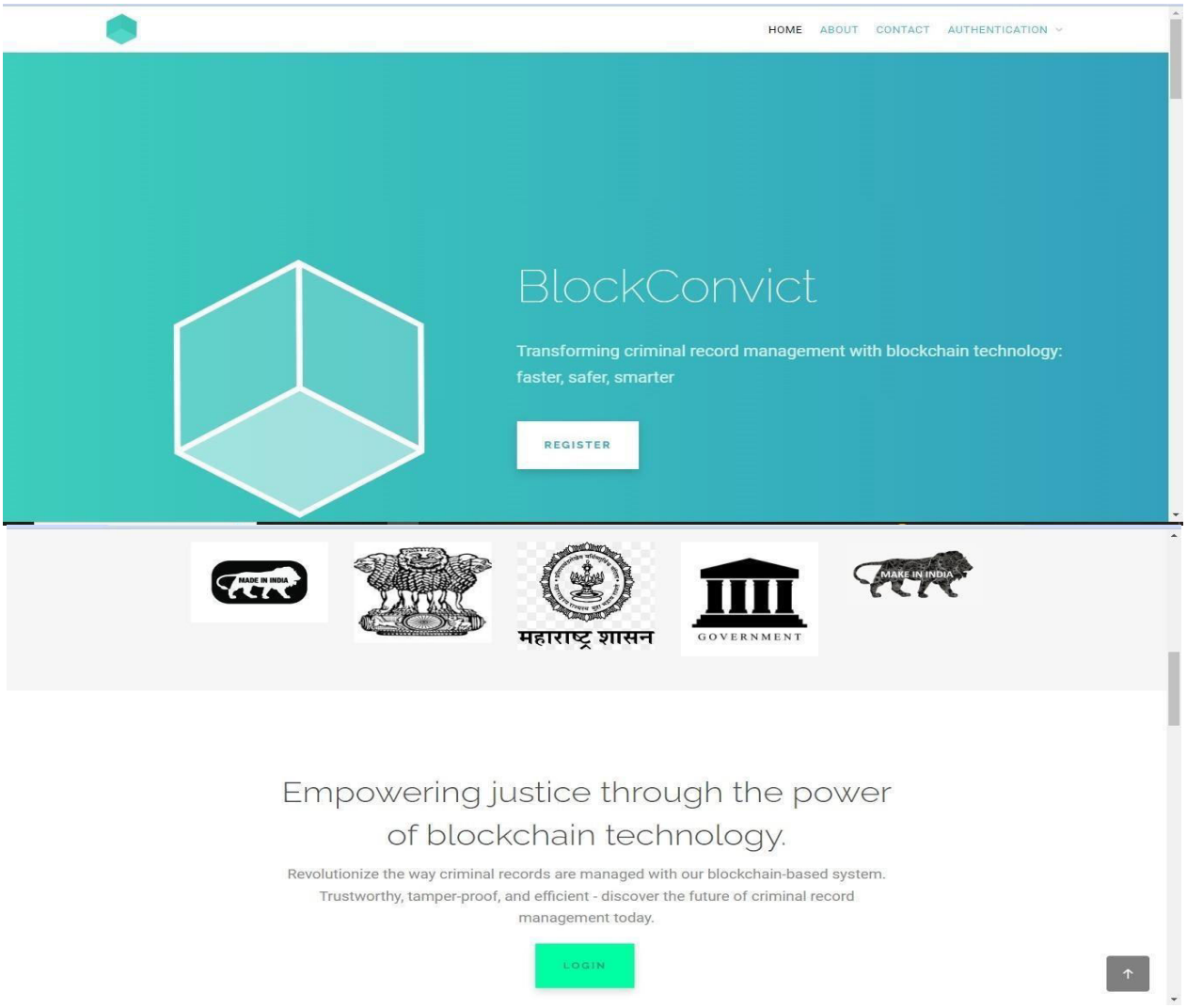
|| Volume 11, Issue 4, April 2023 ||

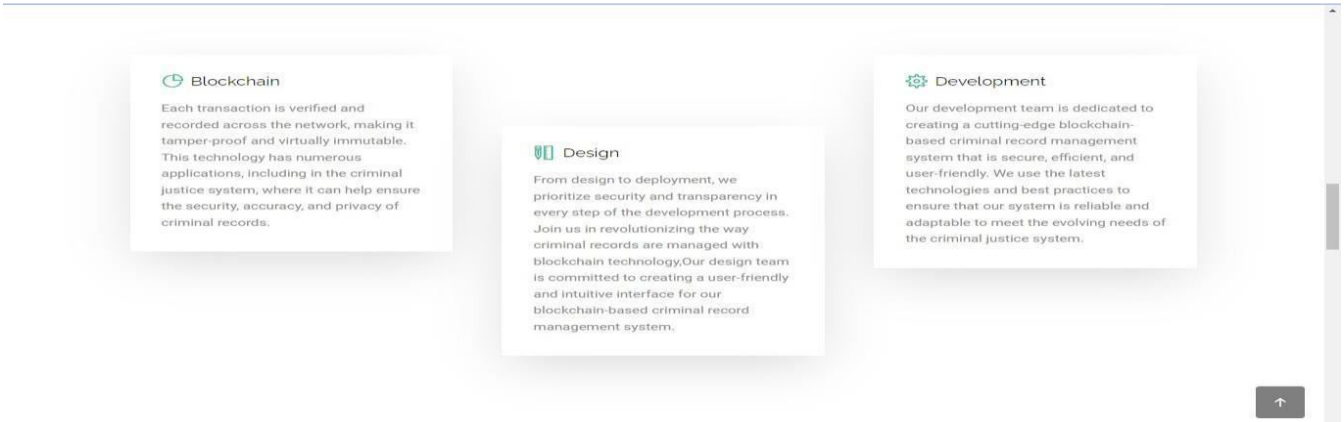
| DOI: 10.15680/IJIRCCE.2023.1104013 |

V. SIMULATION RESULTS

.

This figure will show you how our website look like



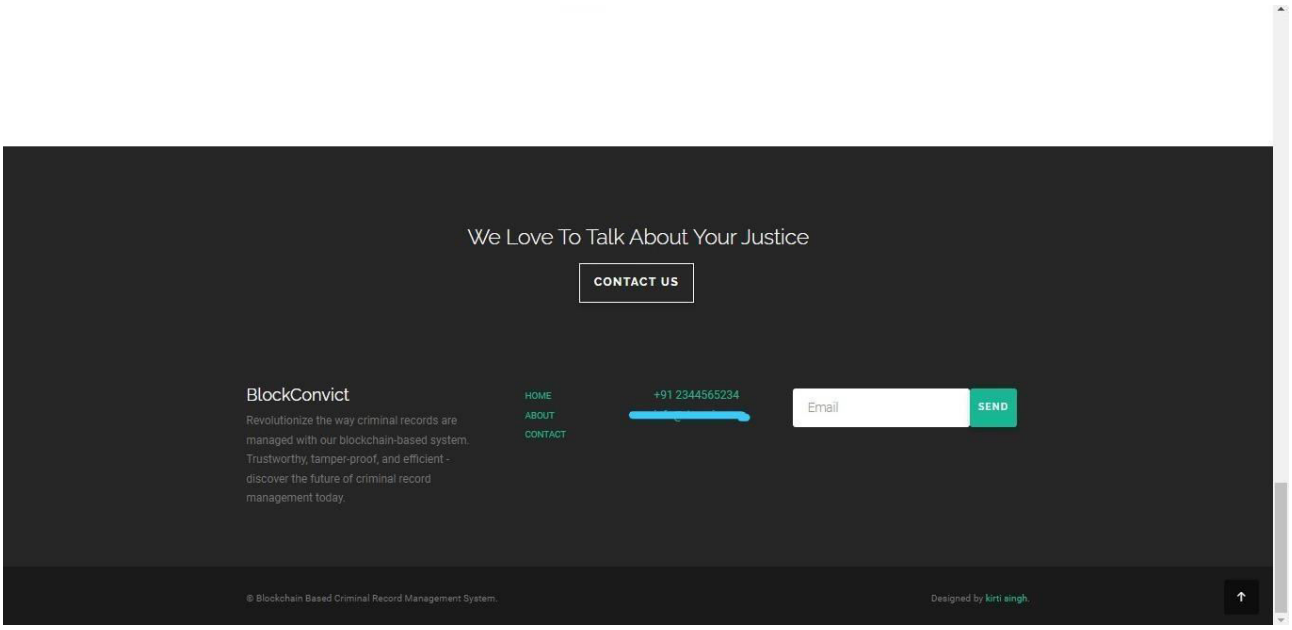


International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 4, April 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1104013 |



VI. CONCLUSION

A blockchain-based criminal record management system has the potential to revolutionize the way criminal records are stored, managed, and accessed. By leveraging the security and immutability of blockchain technology, such a system can ensure the integrity and accuracy of criminal records while enhancing transparency and reducing the risk of tampering or manipulation.

With a decentralized and distributed ledger system, multiple entities and stakeholders can securely access and share criminal records without compromising privacy or confidentiality. This can lead to faster and more efficient background checks, improved collaboration between law enforcement agencies, and more effective crime prevention and detection.

However, the implementation of a blockchain-based criminal record management system also raises important questions about data privacy, security, and accessibility. It is essential to address these concerns and ensure that the system is designed and implemented in a way that protects the rights and interests of all parties involved.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 4, April 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1104013 |

Overall, a blockchain-based criminal record management system has the potential to offer significant benefits to law enforcement agencies, justice systems, and society as a whole. However, careful planning, design, and implementation are crucial to ensure that the system is effective, secure, and ethical.

REFERENCES

1. Anh, D.T.T., Zhang, M., Ooi, B.C., Chen, G.: Untangling blockchain: a data pro- cessing view of blockchain systems. IEEE Trans. Knowledge Data Eng. 30(7), 1366– 1385 (2018)
2. Miles, C.: Blockchain security: what keeps your transaction data safe? https://
3. www.ibm.com/blogs/blockchain/2017/12/blockchain-securitywhat-keeps-your- transaction- data-safe/
4. Ølnes, S., Ubacht , J., Janssen, M.: Blockchain in government: benefits and implications of distributed ledger technology for information sharing (2017)
5. Setiadi, I., Kistijantoro , A.I., Miyaji, A.: Elliptic curve cryptography: algorithms and implementation analysis over coordinate systems. In: 2015 2nd International Conference on Advanced Informatics: Concepts, Theory and Applications (ICAICTA), pp. 1–6. IEEE (2015)

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.379

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details