IJITCE

ISSN 2347- 3657

International Journal of Information Technology & Computer Engineering

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 12, Issue 2, 2024

IMPLEMENTATION OF BLOCK CHAIN TECHNOLOGY IN FORENSIC EVIDENCE SYSTEM

1) Mrs. V SWATI, Associate Professor, Department of CSE, Sreyas Institute of Engineering and Technology, Telangana, India. v.swati@sreyas.ac.in

2) SUKKA. BHANUPRAKASH, Department of CSE, Sreyas Institute of Engineering and Technology, Telangana, India. sukkabhanu123@gmail.com

3) GUGULOTHU. RAHUL NAIK, Department of CSE, Sreyas Institute of Engineering and Technology, Telangana, India. dyrahulnaik22@gmail.com

4) RAMAVATH T. PRABHAS NAIK, Department of CSE, Sreyas Institute of Engineering and Technology, Telangana, India. prabhasnaik81@gmail.com

5) KATTUMULLA. ARCHITHA, Department of CSE, Sreyas Institute of Engineering and Technology, Telangana, India. architharedyk904@gmail.com

Abstract - Crime is an illegal activity that is punished by the government, evidence is required to prove the crime. The evidence gained from a crime place is crucial because it serves as proof of the offense. The digitization of evidence is an urgent necessity. Throughout the investigation process, heterogeneous data formats are generated, and the integrity of sensitive data must be maintained as it passes through the various levels of intermediaries that form the Chain of Evidence (CoE). The evidence needs to be tamper-proof and protected against any alterations. User-friendly interfaces empower registered users to effortlessly upload legal documents and associated information while ensuring end-to-end encryption and secure storage through the Interplanetary File System (IPFS). To build robust systems with immutability, integrity, and legitimacy, blockchain technology is superior. Using blockchain technology, digital evidence can be transferred between parties without a central authority in a transparent manner. We focuses on how blockchain

based solutions can help in building a strong secure system. The system is implemented using Ethereum platform to achieve integrity, immutability transparency as well as tampering can be identified by any one at any time.

Keywords:- Block chain, Document upload, Interplanetary File System (IPFS), Encryption, Transparency, Immutability.

I. INTRODUCTION

The project at hand addresses the crucial need for digitalizing crime evidence in the contemporary digital era, emphasizing the significance of maintaining the integrity of evidence throughout investigations. Tampering and unauthorized access pose serious threats to the reliability of evidence, prompting the exploration of innovative solutions.

ISSN 2347–3657

Volume 12, Issue 2, 2024

Traditional methods of evidence handling face inherent vulnerabilities, making them susceptible to manipulation and compromise. The lack of a robust traceability mechanism in the chain of evidence process raises concerns about the authenticity of the information presented in court. Additionally, the manual and time-consuming document review processes in traditional methods hinder the efficiency of investigations. These drawbacks necessitate a paradigm shift towards more secure and technologically advanced approaches.

The project proposes the integration of blockchain technology to address the shortcomings of traditional methods. Blockchain is like a digital ledger that records transactions securely and transparently. Instead of having all the data in one place, blockchain stores records as blocks of data, each with a unique code called a hash. These blocks are distributed across multiple computers (nodes), making it much harder for anyone to tamper with the data or compromise the entire system. Blockchain offers several advantages.

First, it's decentralized, meaning the data isn't stored in one vulnerable location. Second, it enhances security because the data is stored in encrypted format that's very difficult to alter or hack. Third, it promotes transparency, as all transactions are recorded and visible to authorized users. Fourth, it ensures data immutability, meaning once something is recorded in the blockchain, it can't be easily changed. Finally, it's resilient to failures because even if some nodes go down, others continue to maintain the data.

The project specifically utilizes the Ethereum blockchain for its robust smart contract functionality. Smart contracts are programmable contracts that execute predefined rules and conditions. In this context, smart contracts enhance the security and transparency of the chain of evidence process, enforcing rules related to evidence handling. The decentralized nature of Ethereum contributes to the overall security and reliability of the proposed system, ensuring a trustworthy and tamper-resistant environment for crime evidence.

II. LITERATURE SURVEY

Blockchain technology, originally devised for Bitcoin, has garnered significant attention for its potential beyond crypto currencies. Its immutable and decentralized nature makes it appealing for various industries, including legal and forensic systems. In this literature survey, we explore several scholarly works and reports focusing on the application of block chain in legal chain management, criminal record management, evidence generation, and forensic data sharing.

Mrs. Pallavi R. et al. propose using blockchain to enhance digital forensics by securely storing forensic data across nodes, ensuring transparency and security in investigations. Using Ethereum and smart contracts, dynamic data is stored on a "hot blockchain" and static data on a "cold blockchain." [1].

In "A Blockchain Based Forensic System for IoT Sensors using MQTT Protocol," the authors address security issues in IoT devices using the MQTT protocol by implementing a blockchain-based forensic system. This system ensures evidence

integrity through federated blockchains and uses machine learning for threat assessment, optimizing back-end monitoring resources. [2].

The authors of "Blockchain driven Evidence Management System" secure e-FIR records to prevent unauthorized changes, leveraging the decentralized nature of blockchain. The system ensures data integrity and transparency, utilizing Ethereum smart contracts for secure and verifiable complaint handling.[3].

In "Two-Level Blockchain System for Digital Crime Evidence Management," the authors separate dynamic and static digital evidence to prevent performance degradation. This system ensures secure and reliable management of digital evidence, such as CCTV footage, enhancing investigation integrity.[4].

The authors of "xCRM: Blockchain Interoperable Crime Report Management System" utilize Hyperledger Fabric's Private Data Collection (PDC) and Hyperledger Cacti for secure, decentralized crime report management and international cooperation. It supports anonymous reporting and ensures data privacy and interoperability across various platforms. [5].

Silvia Bonomi, Marco Casini, and Claudio Ciccotelli propose "BCoC: A Blockchain-based Chain of Custody for Evidence Management in Digital Forensics," enhancing the Chain of Custody (CoC) by ensuring evidence integrity and traceability through blockchain. This Ethereum-based prototype automates the CoC process, maintaining unaltered evidence from collection to court.[6].

Lone A. H. and Mir R. N. in "Forensic-chain: Ethereum Blockchain-based Digital Forensics Chain of Custody" guarantee the integrity and authenticity of digital evidence throughout the investigation using Ethereum blockchain. The system provides a comprehensive transaction history, crucial for cybercrime investigations. By leveraging blockchain, it ensures that evidence is tamper-proof and verifiable. This approach enhances the reliability of digital evidence in linking persons to criminal activities. Overall, it aims to strengthen the forensic process and improve the trustworthiness of evidence. [7].

Dr. S. Harihara Gopalan, S. Akila Suba, C. Ashmithashree, A. Gayathri, and V. Jebin Andrews in "Digital Forensics using Blockchain" propose securing the Chain of Custody for digital evidence with blockchain technology, preventing alteration or destruction. This decentralized network ensures data integrity, enhancing the credibility and acceptance of evidence in court.[8].

T. Varshney, N. Sharma, I. Kaushik, and B. Bhushan in "Authentication & Encryption Based Security Services in Blockchain Technology" combine blockchain with IoT to enhance security without centralized authorities. This paper discusses blockchain architecture, its security principles, addressing vulnerabilities, and proposing countermeasures. [9].

Goodell G. and Aste T. in "A Decentralized Digital Identity Architecture" propose a decentralized system for managing digital identities, emphasizing privacy and individual autonomy. It uses distributed ledger

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 12, Issue 2, 2024

technology to support multiple, unrelated identities, avoiding reliance on centralized authorities.[10]

In conclusion, the literature reviewed demonstrates the diverse applications of blockchain technology in legal, forensic, and related domains. From legal document management to criminal record management and evidence generation, blockchain offers innovative solutions to address critical challenges while fostering trust, transparency, and security in the legal and forensic ecosystems.

III. METHODOLOGY

To implement this system, begin by installing and configure an IPFS server for decentralized file storage, ensuring it runs smoothly and configuring settings like CORS as needed. Set up a Flask server for handling business logic and communication with the blockchain and IPFS, implementing APIs for registration, document management, and more. Implement a registration process for Lab, Hospital, Police, Court ensuring authentication and securely storing their information. Allow Lab to upload Evidence through a user-friendly interface, encrypting them before storing on IPFS and recording metadata on the blockchain. Allow Hospital to login and add review. Allow Police to login and add report. Enable Court to log in, review uploaded documents, provide judgments securely. By integrating these components seamlessly, you'll establish a robust legal document management system that leverages blockchain and IPFS technologies for security, transparency, and efficiency in legal proceedings.

A) System Architecture

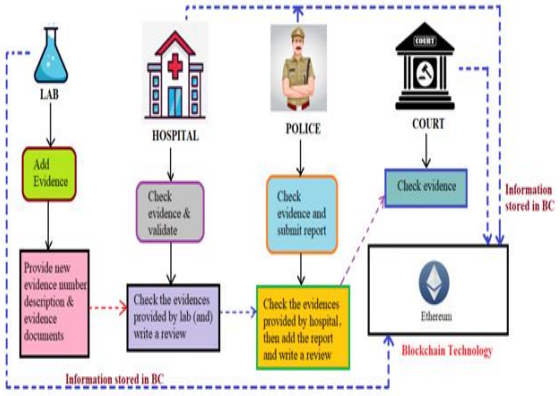

Fig 1: System Architecture

Proposed work

The proposed system is a comprehensive blockchain-based technology for forensic evidence management, designed to enhance security, transparency, and efficiency within the legal framework. It features a user-friendly interface for the secure registration of Labs, Hospitals, Police, and Courts. Each entity is assigned appropriate roles and permissions through robust authentication mechanisms, ensuring accountability and controlled access. Registered users can seamlessly upload legal documents, with encryption applied before storage on the InterPlanetary File System (IPFS) to ensure enhanced security. The system records document metadata and references on the blockchain, guaranteeing transparency and immutability. Courts can securely access these uploaded documents, obtaining the necessary information for review and judgment. By integrating blockchain technology with secure authentication and encryption protocols, the proposed system offers a robust platform for legal record management. This integration fosters trust and

ISSN 2347–3657

Volume 12, Issue 2, 2024

efficiency within the legal system, ensuring that sensitive legal documents are managed with the highest levels of integrity and confidentiality.

B) Modules

1. Starting IPFS Server:

- Install and configure an IPFS server for decentralized file storage.

- Start the IPFS server and ensure it's running properly.

- Configure IPFS settings to work with your application, such as CORS settings.

2. Running the Flask Server:

- Set up a Flask server or any other backend framework for handling business logic and communication with the blockchain and IPFS.

- Start the Flask server and ensure it's listening for incoming requests.

- Implement APIs for registration, document upload/download, and other necessary functionalities.

3. Registering Lab:

- Implement a registration process for Lab.

- Authenticate Lab.

- Store Lab users information securely on the blockchain or in a database.

4. Lab Add Evidence:

- Allow Lab users to log in to the system.

- Provide a user-friendly interface for uploading legal documents and Evidence related information.

- Encrypt documents before uploading them to IPFS for secure storage.

- Record document metadata and references on the blockchain.

5. Registering Hospital:

- Implement a registration process for Hospital.

- Authenticate Hospital and securely store their credentials.

- Provide necessary functionalities for users to manage their accounts.

6. Hospital Add Review:

- Allow registered users to log in to the system.

- Provide a user-friendly interface for adding review.

- Encrypt documents before uploading them to IPFS for secure storage.

- Record document metadata and references on the blockchain.

7. Registering Police:

- Implement a registration process for Police.

- Authenticate Police and securely store their credentials.

- Provide necessary functionalities for users to manage their accounts.

8. Police Add Report:

- Allow registered users to log in to the system.

- Provide a user-friendly interface for adding review.

- Encrypt documents before uploading them to IPFS for secure storage.

- Record document metadata and references on the blockchain.

9. Registering Court:

- Implement a registration process for Court.

- Authenticate Court and securely store their credentials.

- Provide necessary functionalities for users to manage their accounts.

10. Court Review :

- Allow Court to log in to the system using their credentials.

- Provide Court with access to uploaded documents for review.

C) BLOCKCHAIN INTEGRATION

1. Blockchain is a continuously expanding digital ledger that records all transactions in a secure, chronological, and unchangeable manner. It allows for the safe transfer of assets like money, property, and contracts without needing a third-party intermediary.

2. The ledger in a blockchain keeps growing as it adds new transactions permanently. Once a transaction is recorded, it cannot be altered, ensuring a permanent and immutable record.

3. Security is maintained through advanced cryptography, which locks information inside the blockchain, making it highly secure against tampering and unauthorized access.

4. Each transaction is added in a chronological order, meaning every new transaction is recorded after the previous one, ensuring a clear sequence of events.

5. Blockchain technology is versatile and can be used in various fields such as Banking, Finance, Government, Healthcare, Insurance, Media and Entertainment, and Retail, offering secure and efficient ways to manage and transfer information and assets.

IV. RESULTS

Fig 2: Lab Login

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 12, Issue 2, 2024

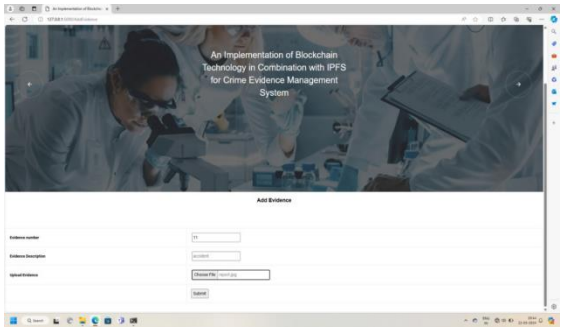

Fig 3: Add Evidence

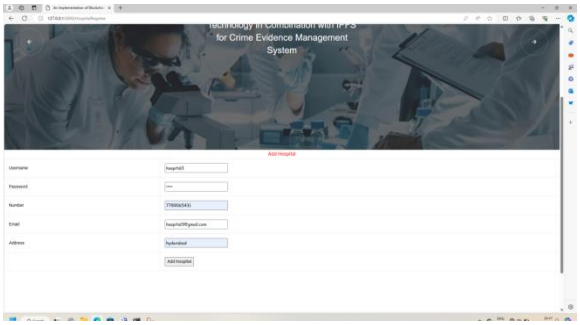

Fig 4: Hospital Registration

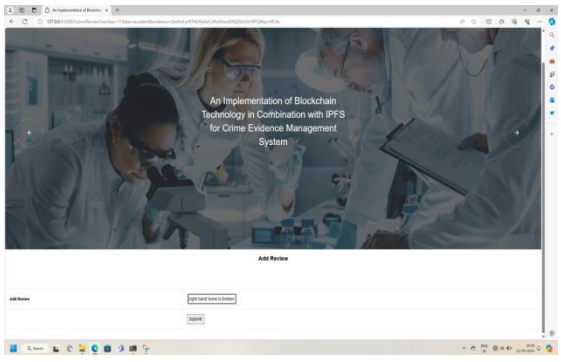

Fig 5: Add Review

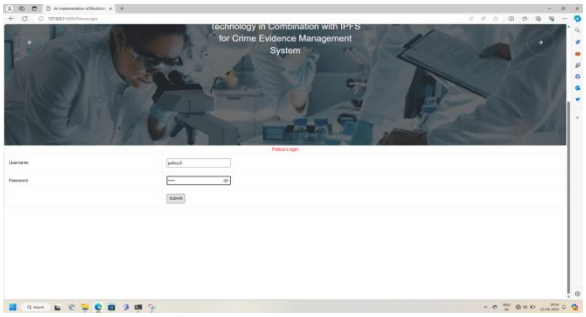

Fig 6: Police Login

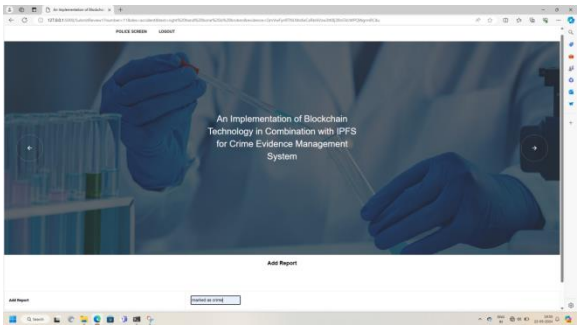

Fig 7: Add Report

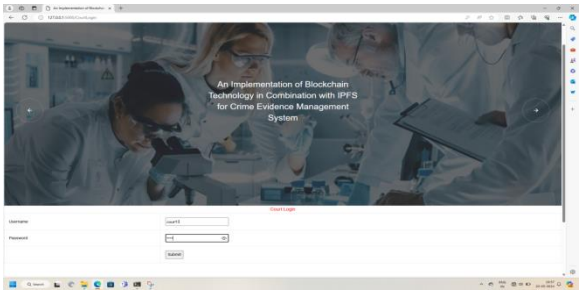

Fig 8: Court Login

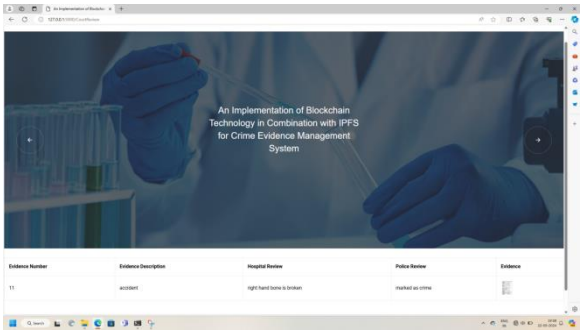

Fig 9: Court Evidence View

V. CONCLUSION

The integration of blockchain technology significantly enhanced the security of crime evidence digitization. The cryptographic features and unique Hashcodes establish a robust defense against tampering, ensuring data integrity. This blockchain implementation ensured a trustworthy Chain of Evidence by maintaining the chronological order of digital evidence. This feature provides investigators with an unaltered and reliable sequence crucial for the integrity of the investigative process. The adoption of blockchain facilitated decentralized, transparent transfer of digital evidence among involved parties. This not only enhances efficiency but also reduces reliance on a central authority, fostering a more agile and collaborative investigative environment. The utilization of smart contracts on the Ethereum blockchain brought transparency to communication protocols. By defining rules and ensuring verifiable interactions, trust is established without the need for third-party intermediaries, contributing to a more secure and streamlined system. Integrated IPFS for secure and distributed evidence file storage, enhancing security through content addressing and Hashcodes, ensuring a tamper-resistant storage solution.

VI. FUTURE SCOPE

The future of blockchain technology in forensic evidence management is promising, with its scalability and interoperability driving broader adoption in forensic settings. Advanced cryptographic techniques and AI algorithms will further enhance the integrity and reliability of evidence. Techniques such as homomorphic encryption and machine learning will ensure privacy during forensic data analysis, protecting sensitive information. Moreover, the integration of blockchain with IoT and augmented reality (AR) technologies will revolutionize real-time forensic data processing and analysis, enabling more accurate and efficient investigations. These advancements will collectively transform forensic science, making it more secure, reliable, and efficient.

REFERENCES

[1] Satoshi Nakamoto " Bitcoin: A peer_to_peer electronic Cash System," May 2008. (online). available: https://bitcoin.org/Bitcoin.pdf

[2] Baygin, N., Baygin, M., & Karakose, M. (2019). Blockchain Technology: Applications, Benefits and Challenges. 2019 1st International Informatics and Software Engineering Conference (UBMYK).

[3] V. Buterin," A next-generation smart contract and decentralised application platform,"White Paper,2014, Ethereum Foundations, Tech.Rep.2014[online].

[4] Zibin Zheng Shaon Xie,"An overview of Blockchain Technology: Architecture,Consensus, and Future Trends",2017; IEEE 6th International Congress on Big Data.

[5] M.Macdonald ,L..Liu_ Thorrold,R.Julien,"The Blockchain: A comparison of Platforms and their Users Beyond Bitcoin" COMS4507_ Advanced Computer and Network Security.

[6] Giuliano Giova, “Improving chain of custody in forensic investigation of electronic digital systems”,

International Journal of Computer Science and Network Security, vol. 11, no. 1, pp. 1–9, 2011.

[7] Auqib Hamid, RoohieNaaz "Forensic-Chain: Ethereum Blockchain Based Digital Forensics Chain of Custody", SPCSJ1(2):21-27 SCSA, 2017 ISSN: 2587-4667.

[8] Shijie Chen, Chengqiang Zhao, Lingling Huang "Study and implementation on the application of blockchain in electronic evidence generation", Elsevier Forensic Science International: Digital Investigation 35 (2020).

[9] Mats Neovius, Magnus Westerlund "Providing Tamper-Resistant Audit Trails for Cloud Forensics with Distributed Ledger based Solutions" IARIA, 2018. ISBN: 978-1-61208-607-1 CLOUD COMPUTING 2018: The Nineth International Conference on Cloud Computing, GRIDs, and Virtualization.

[10] sonali patil,Sarika kadam,Jayashree katti " Security Enchancement of Forensic Evidences Using Blockchain" Proceedings of the Third International Conference on Intelligent Communication Technologies.

[11] Shivani Shetty, Krutika Shinde, Deep Shelke, Ratnakar Garje, Prof. Anita Mahtre, "Crime Evidence Over Blockchain" published in INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT, 9 April 2023, DOI:10.55041/ijsrem18619

[12] Chen Wan; Amjad Mehmood; Maple Carsten; Gregory Epiphaniou; Jaime Lloret, "A Blockchain Based Forensic System for IoT Sensors using MQTT Protocol" published in 2022 9th International Conference on Internet of Things: Systems, Management and Security (IOTSMS), **DOI:** 10.1109/IOTSMS58070.2022.10062190

[13] Shyam Mehta; K. Shantha Kumari; Paras Jain; Harshal Raikwar; Shubham Gore, "Blockchain driven Evidence Management System", published in 2023 3rd International conference on Artificial Intelligence and Signal Processing (AISP), **DOI:** 10.1109/AISP57993.2023.10134799

[14] Donghyo Kim, Sun-Young Ihm, Yunsik Son, "Two-Level Blockchain System for Digital Crime Evidence Management" published in Italian National Conference on Sensors, 27 April 2021, Computer Science, Law, DOI:10.3390/s21093051

[15] Ruhul Amin; Rahat Ahmed Chowdhury; Shah MD Tanjim; Ashraful Islam; Mohammad Shams, "xCRM: Blockchain Interoperable Crime Report Management System By Utilizing Hyperledger Cacti & Private Data Collection (PDC)", published in 2023 International Conference on Next-Generation Computing, IoT and Machine Learning (NCIM), **DOI:** 10.1109/NCIM59001.2023.10212677