ENHANCING FORENSIC EVIDENCE MANAGEMENT WITH BLOCKCHAIN TECHNOLOGY

D. Naga Swetha

Assistant Professor Department of Computer Science and Engineering G.Narayanamma Institute of Technology and Science (for Women)

Telangana, India.

swetha@gnits.ac.in

Abstract

In today's digital age, the authenticity and integrity of evidence play a crucial role in legal, financial, and various other domains. With the advent of block chain technology, a new paradigm for evidence protection has emerged. This paper presents an innovative Forensic Evidence Protection System (EPS) that leverages block chain's inherent characteristics to establish a secure and tamper-resistant framework for safeguarding different forms of evidence. The proposed EPS addresses the challenges associated with evidence tampering, manipulation, and unauthorized access. By utilizing the decentralized and immutable nature of block chain, the system ensures that once evidence is stored within the block chain, it cannot be altered without leaving a trace. Additionally, the system employs cryptographic techniques to maintain the confidentiality of sensitive information while allowing authorized parties to access and verify evidence. The results demonstrated that the EPS offers a robust solution for evidence protection, reducing the risk of tampering and unauthorized alterations. Moreover, the decentralized nature of the block chain ensures that no single point of failure exists, enhancing the overall security of the system.

Keywords: Block Chain, Evidence Protection, Decentralized, Cryptographic Techniques

I INTRODUCTION

The project's primary objective is to establish a robust system for protecting evidence by incorporating block chain technology. This integration aims to enhance the security and reliability of managing sensitive information. Conventional methods relied on centralized databases or physical documentation, which posed vulnerabilities like data tampering and unauthorized alterations due to a lack of robust verification mechanisms. These weaknesses underline the need for a more secure and tamper-proof solution. The project proposes a system that leverages block chain's decentralized structure. It employs cryptographic methods, timestamps, and smart contracts to create a platform that ensures evidence remains tamper-proof, transparent, and authentic throughout its lifecycle. This ensures the integrity and reliability of stored evidence.Ethereum, a prominent blockchain platform, is chosen for its robust features. The project taps into Ethereum's support for smart contracts, its capability for creating decentralized applications (DApps), its active developer community, security enhancements, and compatibility with various blockchain projects. This choice underscores the project's reliance on Ethereum's capabilities to build and enhance the proposed evidence protection system. The choice of Ethereum for implementing the evidence protection system is rooted in its robust features, support for smart contracts and DApp development, active developer community, security enhancements, and compatibility with other blockchain projects. Leveraging these capabilities, the project aims to establish a tamper-proof, transparent, and reliable platform for managing sensitive evidence. From the time the evidence is collected till it's submission in the court, the movement of the evidence throughout the investigation should be traceable. Digitalization of forensic evidence management system saves space and at the same time makes it environment friendly and cost-efficient. Authenticity and legitimacy of CoC make evidence admissible in the court of law. These can be maintained by using block chain technology

II LITERATURE SURVEY

Decentralized Model to Protect Digital Evidence via Smart Contracts Using

Modern legal proceedings heavily rely on digital evidence as a basis for decisions in a variety of contexts, including criminal investigations and civil lawsuits. The decentralized model makes use of smart contracts and blockchain technology to guarantee the integrity,transparency, and immutability of digital evidence. The approach does not require a centralized authority because it makes use of a distributed ledger, which lowers the possibility of data loss or manipulation. Multiple parties participating in the evidence lifecycle can build confidence and accountability thanks to smart contracts' programmable rules. We go over the advantages of employing this architecture, including enhanced auditability, decreased dependency on centralised institutions, and increased data security

Block-DEF: A secure digital evidence framework using blockchain:

A secure digital evidence system should ensure that evidence cannot be tampered with and that private information cannot be leaked. Block chain, a distributed tamper-resistant and privacy-preserving ledger, provides a promising solution for decentralized secure digital evidence systems. However, due to the huge number of digital evidences and the contradiction between the traceability and the privacy of evidence, block chain faces big data and privacy challenges. To solve the above issues, we propose a secure digital evidence framework using block chain (Block-DEF) with a loose coupling structure in which the evidence and the evidence information are maintained separately.

Construction of a Medical Resource Sharing Mechanism Based on Blockchain Technology: Evidence from the Medical Resource Imbalance of China:

Health equity is a very important part of social equity. The outbreak of the novel coronavirus pneumonia (COVID-19) in a short period of time exposed the problems existing in the allocation of medical resources and the response to major public health emergencies in China. By using Kernel density estimation and Data envelopment analysis (DEA). As an important part of the information technology system, blockchain technology is characterized by decentralization and non-tampering. It can realize sharing of medical resources through a mechanism of resource storage, circulation, supervision, and protection.

III EXISTING SYSTEM

The existing work is a conceptual model called "Evidence Chain" that utilizes block chain technology to prevent spoliation of evidence in South Asian countries. The model allows citizens to anonymously upload digital evidence, which is then stored in an immutable and indestructible distributed repository. The ownership of evidence is transferred from authorities to ordinary citizens, which can minimize spoliation of evidence and human rights abuse. The model is theoretically tested against high-profile spoliation of evidence cases from four South Asian developing countries. The existing systems for evidence management and protection in legal and investigative processes face several significant challenges. Traditional evidence management systems are susceptible to tampering and manipulation, as centralized databases can be vulnerable to unauthorized access and alterations. This compromises the integrity of the evidence and undermines its reliability in legal proceedings. Traditional methods often rely on manual processes for establishing and maintaining the chain of custody. This can be time-consuming, error-prone, and lacks the real- time tracking capabilities.

Disadvantages

The existing model allows citizens to upload evidence anonymously.

While block chain technology is utilized for immutability, the specific mechanisms for ensuring the transparency and tamper-resistance of evidence might not be extensively detailed.

Results in delays, miscommunication, and inefficiencies in the legal process.

A breach in security could compromise the integrity of the evidence, leading to potential miscarriages of justice. The process is time-consuming, prone to errors, and may lack real-time updates, making it challenging to ensure the secure and transparent transfer of evidence.

IV PROBLEM STATEMENT

The existing systems for evidence management in legal and investigative processes often face various drawbacks, impacting their efficiency, security, and overall effectiveness. Many traditional systems rely on centralized databases, making them vulnerable to hacking, unauthorized access, and manipulation. Traditional systems may lack robust security measures to protect sensitive information. Without advanced encryption and access controls, the risk of data breaches and unauthorized disclosure of evidence remains high. Some existing systems may face challenges in handling a large volume of evidence or adapting to the increasing complexity of legal cases. Evidence management is critical in the field of forensic science. Chain of Custody (CoC) is the documentation of the evidences handled throughout the investigation in chronological order

V PROPOSED SYSTEM

The Forensic Evidence Protection System (FEPS) presented in this paper harnesses the unique attributes of block chain technology to create a secure, tamper-proof, and transparent environment for safeguarding evidence across a spectrum of applications. The system offers a comprehensive set of features that address the challenges associated with evidence tampering, data manipulation, and unauthorized access, while also promoting efficient evidence handling and verification. The

proposed Evidence Protection System introduces a paradigm shift in evidence management by harnessing the capabilities of block chain technology. Its robust architecture ensures the integrity, authenticity, and accessibility of evidence, while its automation and security features streamline evidence handling processes. With applications across various domains, the EPS holds the potential to redefine how evidence is protected, shared, and trusted in our increasingly digital and interconnected world. The proposed project leveraging block chain technology to address these issues. The proposed FEPS employs a decentralized and distributed block chain ledger to securely store, timestamp, and verify various types of evidence. Through cryptographic techniques, digital timestamps are generated, creating an immutable record of the evidence on the blockchain. This decentralized approach eliminates the vulnerabilities

Associated with centralized systems, ensuring tamper-proof storage and transparent access.

Advantages

Eliminates the risk of unauthorized access, manipulation, or tampering.

Ensures a secure and transparent transfer of evidence.

Simplifies the verification process and strengthens the credibility of evidence presented in legal proceedings.

It promotes interoperability and avoids disruptions in the legal process.

Block chain's transparent and decentralized nature ensures that all changes and transactions related to evidence are visible and traceable.

By ensuring evidence authenticity, transparency, security, and automated processes, the EPS contributes to more credible and fostering trust and reliability across various sectors.

V IMPLEMENTATION

User Signup: This module allows individuals to create accounts within the system. Users provide necessary details, possibly including personal information, credentials (username, password), and any additional required data. Upon successful registration, their information is stored securely within the system, likely leveraging block chain for data integrity.

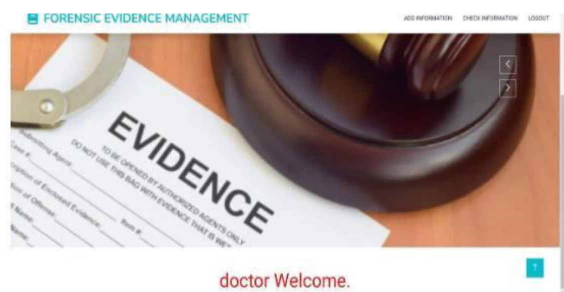
User Sign-in: Once registered, users can sign in using their credentials. This module verifies the provided information against stored records to authenticate users. Upon successful authentication, users gain access to the system's functionalities based on their assigned permissions and roles.

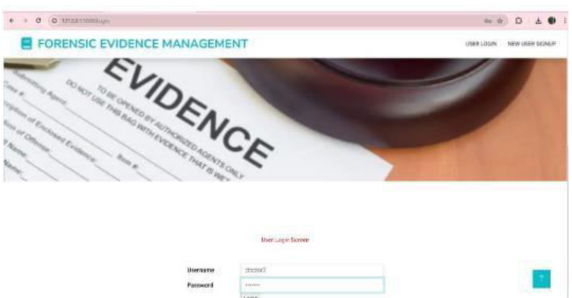
Add Information: This module enables users to input or upload evidence-related information into the system. It could involve uploading documents, entering data, or

attaching files relevant to the evidence being managed. The information added goes through processes ensuring its authenticity, immutability, and secure storage, often leveraging blockchain's capabilities.

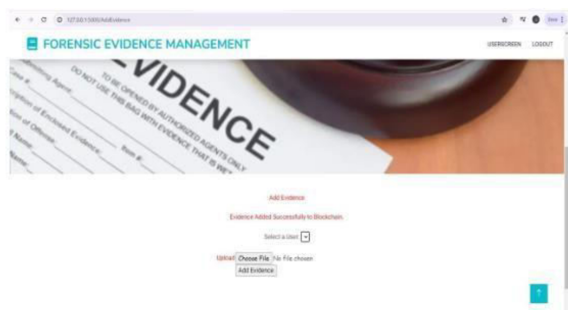
Check Information: Users utilize this module to access and verify information stored within the system. It provides them with the ability to search, retrieve, and view specific evidence or related data. The module ensures transparent access to authorized users while maintaining the security and integrity of the stored information. The integration of these modules within the system ensures a comprehensive and secure approach to managing evidence while leveraging block chain technology to maintain the integrity and security of the stored information

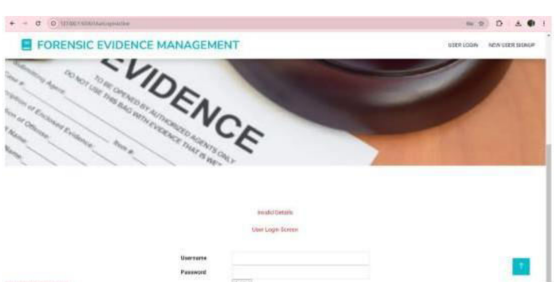
VII RESULTS



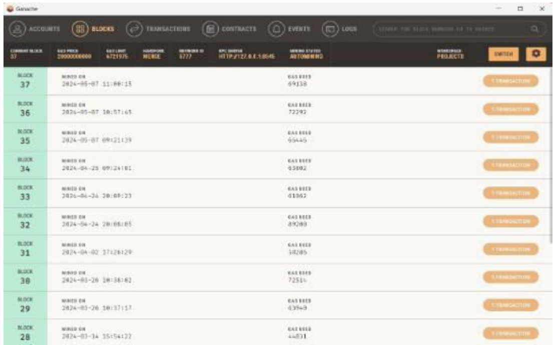


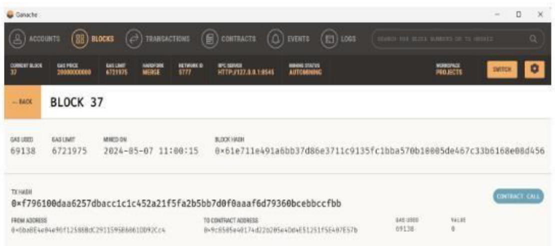
Screenshort-8.1.3





\





VIII CONCLUSION

The conclusion outlines the successful implementation and testing phases of the evidence protection system based on block chain technology. It signifies that the system has been developed, deployed, and subjected to rigorous testing to validate its functionality and performance. The project emphasizes how block chain technology effectively ensures the creation of tamper-proof evidence records. It highlights the system's ability to enhance security by utilizing block chain’s inherent features such as immutability, cryptographic security, transparency, and reliability in securing evidence. The conclusion provides a summary of the project's achievements and positive outcomes. It could include milestones reached during the development phase, showcasing the successful creation of a decentralized and transparent system for managing evidence, indicating a step forward from traditional methods. It highlights the improvements brought about by utilizing block chain technology in evidence management. These improvements encompass enhanced integrity (unalterable records),heightened security (through cryptographic measures), and improved accessibility (transparent access for authorized users).

REFERENCES

Sumit Kumar Rana, Arun Kumar Rana, Sanjeev Kumar Rana, Vishnu Sharma, Umesh KumarLilhore, Osamah Ibrahim Khalaf, Antonino Galletta, "Decentralized Model to Protect Digital Evidence via Smart Contracts Using Layer 2 Polygon Blockchain", IEEE Access, vol.11, pp.83289-83300, 2023.

2. Z. Tian, M. Li, M. Qiu, Y. Sun and S. Su, "Block-DEF: A secure digital evidence framework using blockchain", Inf. Sci., vol. 491, pp. 151-165, Jul. 2019.

3. Hu Liu, Yuxuan Liu, “Construction of a Medical Resource Sharing Mechanism Based on Blockchain Technology: Evidence from the Medical Resource Imbalance of China” published in Healthcare 1 January 2021, DOI:10.3390/healthcare9010052

4. Ana Nieto, Rodrigo Roman, and Javier Lopez, “Digital Witness: Safeguarding Digital Evidence by Using Secure Architectures in Personal Devices,” IEEE Network, vol. 30, no. 6 pp. 34 – 41, 2016.

5. Akinseye Oluwaseyitan Charles, Abiodun Oguntimilehin, Oniyide Alabi Bello, “Forensic Evidence Security System using Blockchain Technology”, published in International Journal of Engineering Trends and Technology, Volume 71 Issue 8, 143-151, August 2023, Available at https://doi.org/10.14445/22315381/IJETT-V71I8P212

6. M. K. Pandya, S. Homayoun, and A. Dehghantanha, ‘‘Forensics investigation of openflow-based SDN platforms,’’ in Advances in Information Security, vol. 70. Cham, Switzerland:Springer, 2018, pp. 281–296.

7. T. Chin and K. Xiong, ‘‘A forensic methodology for software-defined network switches,’’ in Proc. IFIP Int. Conf. Digit. Forensics, 2017, pp. 97–110.

8. Y. Xie, D. Feng, X. Liao, and L. Qin, ‘‘Efficient monitoring and forensic analysis via accurate network-attached provenance collection with minimal storage overhead,’’ Digit. Invest., vol. 26, pp. 19–28, Sep. 2018.

9. B. Zhao, P. Fan, and M. Ni, ‘‘Mchain: A blockchain-based VM measurements secure storage approach in IaaS cloud with enhanced integrity and controllability,’’ IEEE Access, vol. 6, pp.43758–43769, 2018