IES International Journal of Multidisciplinary Engineering Research

Forensic Evidence Security System

Aysha Dilna [1], Ananya M.S [2], Mohammed Ziyaan [3], Faraz P A[4], Athira A K [5]

[1, 2, 3, 4] *Student, Department of Computer Science and Engineering, IES College of Engineering, Thrissur, Kerala, India*

[5] *Assistant Professor, Department of Computer Science and Engineering, IES College of Engineering, Thrissur, Kerala, India*

Email_id: ayshadilna11@gmail.com, anua48843@gmail.com, ziyaan8132@gmail.com, farazpa773@gmail.com, athiraak@iesce.info

Abstract

Data security is vital in forensic investigations, where data integrity and provenance are essential. Blockchain, specifically on the Ethereum platform, offers a decentralized and tamper-resistant solution, ensuring forensic data remains immutable and traceable across the investigative chain. This technology helps maintain trust and transparency, as any tampering becomes detectable.Additionally, a public-facing chatbot provides real-time information on forensic standards, enhancing public understanding and trust in evidence handling practices. This dual approach strengthens security and accessibility,fostering greater accountability in forensic processes.

Keywords: Forensic Evidence, Blockchain, Digital Security, Smart Contracts, Chain of Custody, Evidence Management

DOI: https://doi.org/10.5281/zenodo.15153060

1. Introduction

In forensic investigations, safeguarding the integrity and security of evidence is paramount, as any compromise can directly impact the reliability and admissibility of findings. With the rapid increase in cybercrime, the need to protect forensic data has become more pressing, especially given the sensitive and confidential nature of this information. Forensic evidence typically passes through multiple intermediaries, including pathology labs, medical experts, and police departments, each handling, analysing, or storing data at different stages. Ensuring data remains intact, authentic, and secure at each stage of this chain is vital to maintaining public trust and upholding transparency within legal proceedings. A promising solution to this challenge is blockchain technology, which offers a decentralized and tamper resistant framework formanaging data.By implementing a blockchain systemon platforms like Ethereum, forensic data can be handled in a way that ensures immutability—any alteration of records is detectable, making tampering almost impossible without leaving a trace. This transparency is especially valuable in forensic investigations, where the credibility of evidence is critical to the outcome of cases. Each piece of forensic data entered into the blockchain is timestamped, securely transferred, and recorded across multiple nodes, creating an unchangeable log that preserves data provenance from the point of collection through to court proceedings. Beyond securing data, blockchain technology also enhances traceability, enabling each interaction with the data to be tracked and verified. This aspect is essential for evidence that changes hands multiple times; every time a forensic report is accessed or shared, the blockchain records these actions, ensuring that a clear chain of custody is

maintained. This secure structure provides law enforcement and judicial bodies with confidence that the evidence presented has not been altered or compromised, increasing the reliability of forensic evidence and findings. To further support transparency and public awareness, a public-facing chatbot module complements the blockchain system. This chatbot serves as an accessible resource, providing real-time information on the forensic process, including rules, regulations, and standards for evidence handling. By answering questions and offering clear guidance, the chatbot helps the public understand the rigorous protocols in place to protect evidence and maintain integrity. This added layer of openness aims to build trust, as individuals can gain insights into how evidence is managed and secured in the justice system. Together ,the integration of blockchain for secure data handling and a chatbot for accessible information creates a comprehensive approach to modern forensic investigations. This dual strategy not only improves the security and transparency of forensic data but also fosters a sense of accountability and trust within the legal system. By combining advanced digital security with public accessibility, this system addresses the complexities of modern forensic investigations in an era of increasing digital threats, helping ensure justice is served with the highest level of integrity.

2. Literature Review

Blockchain-based chains of custody ensure tamper-proof integrity and transparency of forensic evidence but face challenges with scalability and regulatory acceptance [1]. The integration of AES and PKI encryption enhances data security, yet the complexity of implementation and key management remains a drawback [2].AI-driven anomaly detection offers real-time monitoring for unauthorized access but is constrained by the quality of training data, often leading to false positives or negatives [3]. Smart contracts automate evidence handling processes, minimizing human error, but lack flexibility and may contain code vulnerabilities [4] Blockchain improves accountability and integrity in forensic processes through immutable records, though it incurs high computational and storage costs [5]. A hybrid system combining blockchain, cloud, and encryption optimizes cost and latency but introduces design complexity [6].Metadata analysis enhance strace ability and manipulation detection, although it may require additional resources and might miss subtle alterations [7].A holistic security framework integrating blockchain, encryption, and AI provides comprehensive protection but poses high implementation costs and complexity [8]. Using blockchain in forensic labs addresses scalability and regulatory compliance issues but requires substantial upfront investment and adherence to jurisdictional laws [9].Emphasizing blockchain's legal admissibility and educating legal professionals promotes its application, yet adoption is slow, and training needs are high [10].Secure evidence transfer protocols offer encrypted and tamper-proof transfers but may add latency and complexity to workflows [11]. AI'srolein automating forensic analysis boosts efficiency but relies on robust algorithms and faces challenges in courtroom interpretation [12]. Standardized blockchain practices ensure consistency and reliability but encounter difficulties in widespread adoption across jurisdictions [13].Integrating blockchain, encryption, and AI addresses individual technology limitations but increases system complexity and raises interoperability concerns[14].Finally ,transparent and secure evidence tracking using blockchain bolsters credibility, although it imposes significant storage and computational overheads. Together, these innovations showcase significant advancements in forensic security while presenting challenges that need to be addressed for widespread adoption and optimization [15].Collectively, these studies address challenges like legal

compliance, scalability, and interoperability, showcasing blockchain's transformative potential in forensic investigations.

3.1 Proposed System

The proposed system using the Blockchain technology, combined with encryption and AI, significantly enhances the management of forensic evidence. Blockchain's immutable ledger ensures secure storage and tracking, while encryption prevents unauthorized access, and AI detects anomalies. This decentralized framework eliminates single points of failure, improves data integrity, and automates evidence handling through smart contracts, reducing human error. The proposed system uses blockchain technology to ensure the security, integrity, and transparency of forensic evidence in the criminal justice system. By storing evidence in encrypted form and controlling access through cryptographic keys, the system prevents unauthorized access and tampering, while maintaining transparency for the police department, forensic staff, and the public.

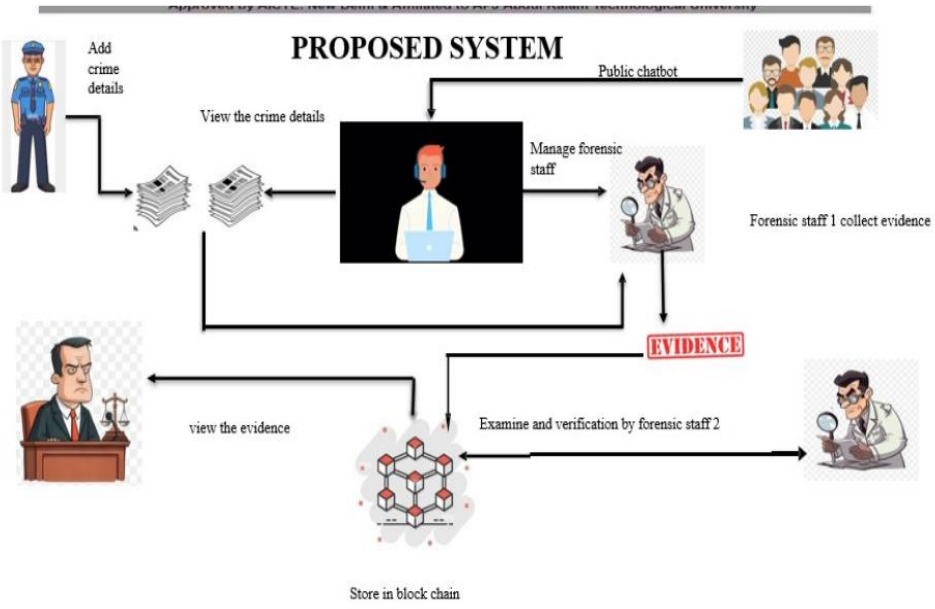

Figure 1: Proposed System

The proposed system leverages blockchain technology to ensure the security, integrity, and transparency of forensic evidence within the criminal justice system. By storing evidence in an encrypted format and regulating access through cryptographic keys, the system prevents unauthorized access and tampering while maintaining transparency for the police department, forensic staff, and the public. The system comprises four main modules: the Police Department, Forensic Staff, the Court System, and the Public Chatbot. The process begins with the Police Department, where a designated police officer logs the crime details into the system, including witness statements and collected evidence. The officer then creates an investigation evidence forwards it to the system administrator for review and then which is shared with forensic teams and the court for further examination. In the Forensic Module, two forensic staff members play a crucial role in evidence collection and verification. Forensic Staff 1 examines the crime scene or victim and collects key evidence, such as biological samples, fingerprints, or digital records. This

evidence is then securely transferred to Forensic Staff 2, who thoroughly examines and verifies the collected data. After verification, the forensic evidence are securely stored in the blockchain, ensuring their immutability and protecting them from unauthorized modifications. The Court System is responsible for validating forensic evidence and ensuring their authenticity. Upon receiving the verified forensic evidence, the court retrieves it directly from the blockchain and viewing for maintain transparency and prevent any alterations. Once the court satisfied, it approves the evidence and permanently stores it in the blockchain, making it accessible only to authorized legal stakeholders, including judges, lawyers, and defense teams. This ensures that all judicial decisions are based on verified, tamper-proof evidence. Finally, the Public Chatbot serves as an interactive platform that provides secure and precise case-related information to the public. Using an advanced question-answering system powered by extensive case data, the chatbot delivers accurate and efficient responses about ongoing investigations. This feature enhances transparency and public trust while ensuring that sensitive case details remain protected. By integrating blockchain technology, the proposed system enhances collaboration between law enforcement agencies, forensic experts, and the judiciary. It ensures the reliability of forensic evidence, prevents unauthorized access or tampering, and provides a transparent and secure platform for managing crime investigations. This approach strengthens the integrity of the judicial system while fostering public confidence in the criminal justice process.

3.2. Police Department:

This module manages the initial stages of investigations. When a crime is reported, a designated officer collects information, interviews witnesses, and gathers evidence to build the case. The findings are compiled into a detailed investigation report, which is reviewed by an administrative officer for accuracy and completeness before being forwarded to forensic teams and the court. Blockchain integration ensures an immutable log of each step, enhancing transparency and accountability.

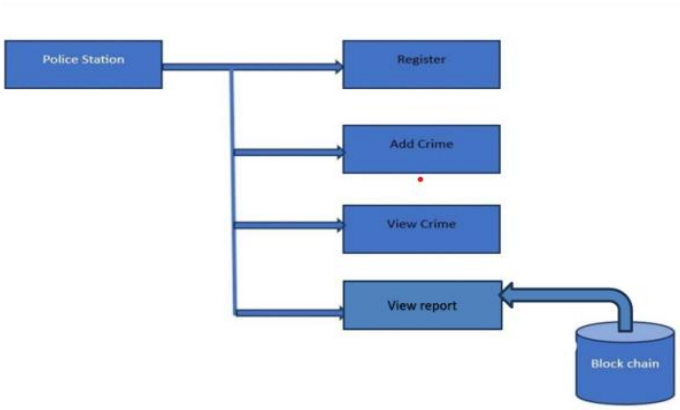

Figure 2: Police Department Module

3.3.Forensic Staff 1:

Forensic Staff 1 collects evidence from the crime scene, such as biological samples, fingerprints, or digital evidence, recording detailed observations, methodologies used, and preliminary conclusions. The evidence is then sent to Forensic Staff 2 for meticulous verification, which includes cross- checking findings and re-evaluating

samples. Once verified, the evidence and report are securely added to the blockchain, ensuring immutability and enhancing collaboration and reliability in forensic processes.

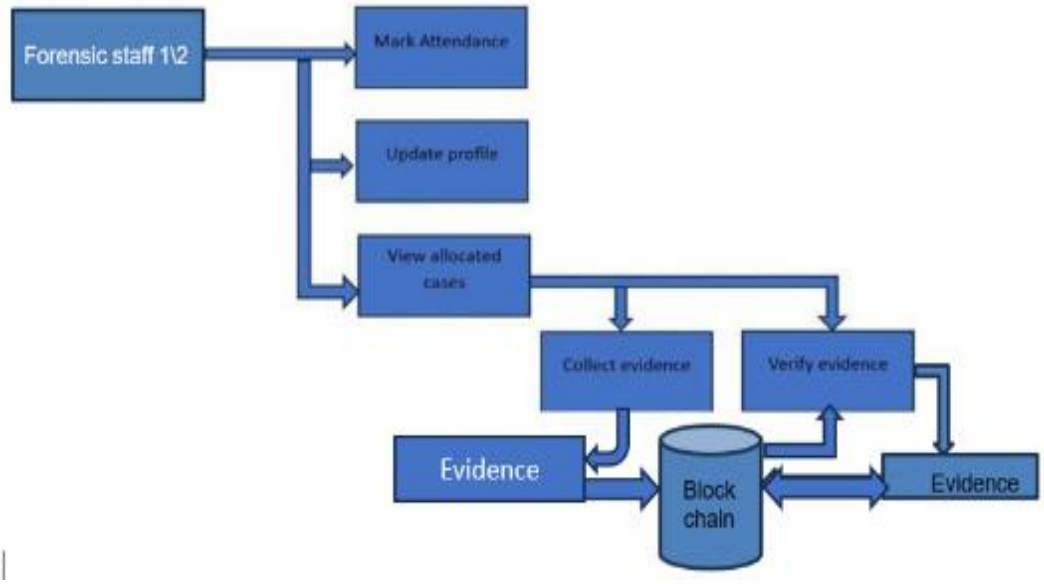

Figure 3: Forensic Staff Module

3.4. Court:

The court module ensures the integrity of the judicial process by validating forensic reports. Upon receiving verified reports, the court examines their authenticity and relevance, requesting clarifications or additional evidence if needed. Creating at amper-proof record accessible to all stakeholders. This module upholds fairness and transparency in trials.

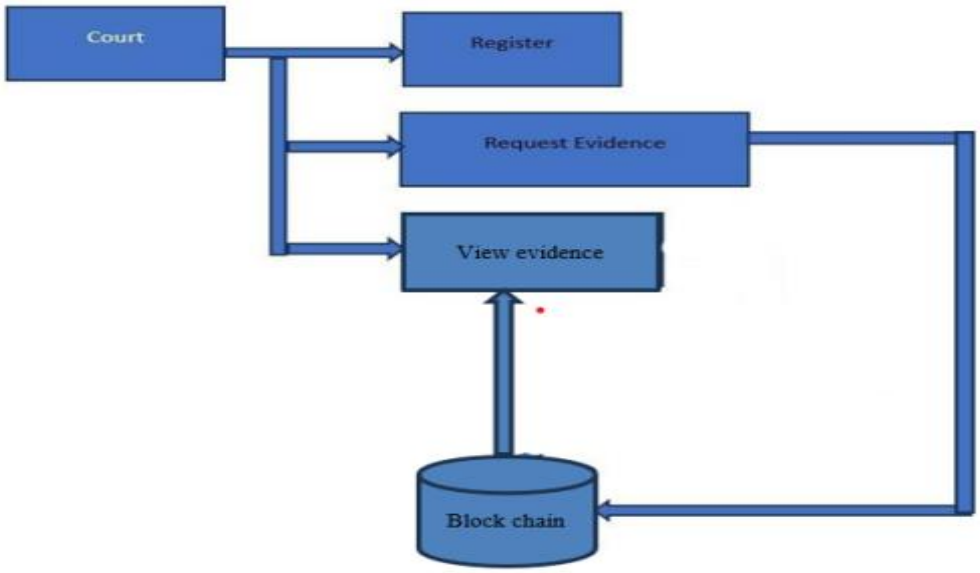

Figure 4: Court Module

3.5 Public

The public module connects the community with the criminal justice system through a chatbot that provides secure, accurate responses to queries about case statuses, forensic procedures, and legal information. Using advanced natural language processing, it ensures efficient information retrieval while maintaining data confidentiality. This module fosters transparency, trust, and public engagement in the justice process. LSTM (Long Short- Term Memory) technology helps reduce the risk of data alteration or manipulation in forensic investigations by analyzing time-series data, such as logs, to detect anomalies or inconsistencies that may indicate tampering. By learning patterns in sequential data, LSTM models can flagir regularities and help maintain the integrity of evidence. Additionally, LSTM enhances privacy by detecting and anonymizing sensitive information, such as personally identifiable data, in digital evidence while preserving its context. It can also work with encryption techniques to protect data during storage and transfer, ensuring secure and private handling of forensic evidence. The LSTM technology for reduces the risk of data alteration or manipulation, a key concern in forensic investigations and to enhance the privacy of digital evidence.

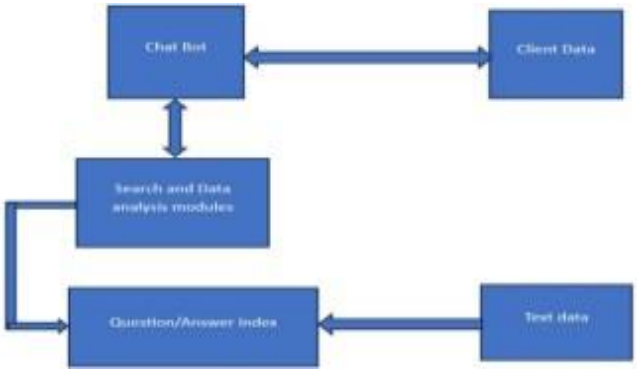

Figure 5: Public Module

4. Implementation of forensic evidence system

The implementation of the proposed blockchain-based forensic evidence managment application requires a clear specification of hardware, software, and functional requirements to ensure an effective, secure, and user-friendly system.

4.1 Hardware Requirements:

- Processor: Intel Pentium Core i5 or higher, to ensure sufficient processing power for handling multiple transactions and data processing.
- Primary Memory: 8GB RAM or higher, to support real-time tracking, transaction processing, and seamless user interaction.
- Storage: 500 GB hard disk or higher, to accommodate data storage for records, logs, and other necessary files.

4.2 Software Requirements

- Operating System: Windows 7 Ultimate or above, to ensure compatibility with required development tools and software environments.

- Front-End Development: HTML, Flutter widgets, CSS, Bootstrap for creating an accessible and responsive user interface.
- Back-End Development: Python, Django, and MySQL Server for handling data processing, server-side logic, and database management.
- Blockchain Development: Truffle Suite and Ganache, to facilitate blockchain and smart contract development, deployment, and testing.
- App Development: Python and Tart are used for app development.
- Development Tools: Pycharm or any preferred Integrated Development Environment (IDE) for efficient coding and debugging.

4.3.1 Police Station

This module manages the initial stages of the investigation process. When a crime is reported, a designated police officer is assigned to the case, logs the crime into the system, and provides all relevant details, including collected evidence and witness statements. The administrative officer then reviews the submitted information, verifies its accuracy, and compiles a detailed investigation report. This evidence is forwarded to forensic teams and the court for further examination. The module integrates with blockchain, allowing police officers to securely access and review case details while ensuring an immutable record for accountability and transparency.

4.3.2 Forensic Department

This module encompasses the roles of forensic staff involved in the collection and analysis of forensic evidence. When a crime is reported, forensic staff member 1 collects evidence, such as biological samples, fingerprints, or digital data, and securely stores it in the blockchain. Forensic staff member 2 then retrieves the stored evidence from the blockchain for rechecking and verification. During this process, if staff member 2 detects any errors or inconsistencies in the evidence, they send a text message to staff member 1, highlighting the issue. When staff member 1 logs in, they receive the error notification and take the necessary steps to correct the discrepancies. Once the corrections are made, the updated evidence is securely added back to the blockchain. Staff member 2 then retrieves the corrected evidence again for final verification. After ensuring its accuracy and completeness, the verified evidence is securely stored in the blockchain, maintaining the integrity and reliability of forensic data. This system enhances collaboration among forensic professionals while ensuring that all evidence remains accurate and tamper-proof access protocols. Upon approval, the court retrieves the verified forensic evidence directly from the blockchain to ensure authenticity and relevance to the case.The validated evidence remains securely stored on the blockchain and is accessed by authorized legal stakeholders, including judges, lawyers, and defense teams. This module ensures that all parties involved in the judicial process rely on the same verified information, maintaining the integrity of the judicial system and facilitating fair trials.

4.3.4 Public Chatbot:

The public module serves as an interface between the criminal justice system andthe community, providing transparent and accessible forensic information. It includes achatbot designed to assist the public in accessing forensic evidence. This chatbot utilizes advanced natural language processing capabilities to analyze client queries and provide precise, relevant responses based on a comprehensive question-answer index supported by extensive

text data. It ensures secure and efficient information retrieval, allowing users to inquire about case statuses, forensic procedures, and general legal information. Additionally, the public module promotes transparency by providing controlled access to relevant information without compromising sensitive data, fostering trust and engagement with the community.

To further enhance security and data integrity, the system incorporates Long Short-Term Memory (LSTM) technology. LSTM helps reduce the risk of data alteration or manipulation by analyzing time-series data, such as forensic logs, to detect anomalies or inconsistencies that may indicate tampering. By learning patterns in sequential data, LSTM models can flag irregularities, ensuring the authenticity of forensic evidence. Additionally, LSTM enhances privacy by detecting and anonymizing sensitive information, such as personally identifiable data, within digital evidence while preserving its contextuall meaning. It can also work alongside encryption techniques to protect forensic data during storage and transfer, ensuring secure and private handling. The integration of LSTM technology strengthens the forensic investigation process by safeguarding evidence from manipulation and enhancing the privacy and reliability of digital records.

5. Result and discussion

The forensic evidence security system ensures data integrity, security, and transparency in investigations by integrating blockchain technology. It establishes an immutable chain of custody, preventing unauthorized modifications and ensuring evidence authenticity. All modules—including the police, forensic staff, court, and chatbot—function seamlessly to enhance secure data handling. The system records every transaction on the blockchain, creating a tamper-proof audit trail. Cryptographic hashing detects unauthorized alterations, and forensic staff modules ensure accurate evidence collection. The court module validates forensic records, ensuring legal admissibility. A chatbot enhances public awareness while maintaining confidentiality. Performance testing confirms the system efficiently handles large forensic data volumes, eliminating single points of failure and resisting cyber threats. By leveraging blockchain, cryptographic security, and automated verification, the system enhances reliability, accountability, and efficiency, providing a robust framework for forensic investigations.

6. Performance

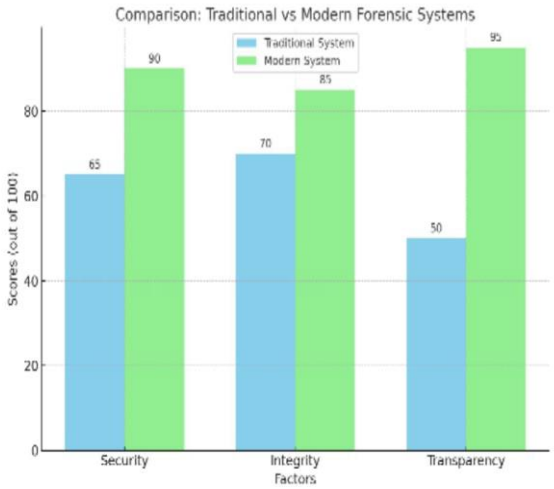

Figure 6: Performance

7. Conclusion

An Ethereum-based blockchain system offers a secure, transparent, and tamper-proof solution for forensic evidence management, ensuring data integrity, traceability, and immutability. By recording transactions immutably, it prevents unauthorized modifications, reducing risks associated with traditional centralized databases. Blockchain's decentralized structure enhances security, making forensic records more reliable and admissiblein court. Smart contracts automate compliance with legal standards, minimizing human errors and ensuring only authorized personnel can access or modify forensic data. Additionally, an AI-powered chatbot improves public access to forensic knowledge, enhancing transparency and trust in legal processes. The system provides fully auditable trail ofevidence transactions, reducing disputes and fraudulent claims. Its interoperability with law enforcement databases and forensic laboratories enables seamless yet secure information exchange. This blockchain-based approach revolutionizes forensic investigations by safe guarding evidence, improving efficiency, and reinforcing the credibility of the legal process.

8. References

[1]. M. Khezr,"Sec-Health: ABlockchain-Based Protocol for Securing Health Records," IEEE Access, 2019.

[2]. Q. Zhang,"A Study of a Blockchain-Based Judicial Evidence Preservation Scheme, "Journal of Forensic Sciences, 2020.

[3]. N. Singh,"Blockchain based cloud computing: Architecture and research challenge, "Journal of Cloud Computing, 2020.

[4]. F S. Patel,"Security Enhancement of Forensic Evidence Using Blockchain, "Journal of Information Security and Applications, 2021.

[5]. A. Rahman,"Decentralized Model to Protect Digital Evidence via Smart Contracts Using Layer 2 Polygon Blockchain," International Journal of Digital Evidence Management, 2021.

[6]. W. Wang and D. T. Hoang, "A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks," IEEE Access, 2016,

[7]. Z. Zheng, S. Xie, H. Dai, X. Chen, and H.Wang, "An overview of Blockchain Technology: Architecture, Consensus, and Future Trends, "IEEE International Congress on Big Data,2017.

[8]. G. Giova, "Improving chain of custody in forensic investigation of electronic digital systems," International Journal of Computer Science and Network Security, 2011.

[9]. M. Macdonald, L. Liu-Thorrold, and R. Julien, " The Blockchain: A comparison of platforms and their users beyond Bitcoin," Advanced Computer and Network Security, 2017.

[10]. K. Zile and R. Strazdina, " Block chain and Use Cases and Their Feasibility, "Applied Computer Systems, Riga Technical University, May 2018.