Blockchain Based Framework for Securing Digital Evidence

Deevi Radha Rani, Tavva Karthik, Tammineni Narasimha and Kola Rajesh
Department of Advanced Computer Science and Engineering, Vignan's Foundation for Science, Technology & Research (Deemed to be University), Vadlamudi, Guntur (Dt), 522213, Andhra Pradesh, India

Keywords: Blockchain, Chain of Custody, Integrity, Ethereum, Smart Contracts.

Abstract: Digital evidence's traceability and integrity are essential for maintaining credibility and dependability in forensic investigations and court cases. Conventional approaches to chain of custody management frequently encounter issues like inefficiency, tampering, and a lack of transparency. By offering a decentralized, unchangeable, and impenetrable platform for managing digital evidence, blockchain technology offers a revolutionary alternative. This paper proposes a blockchain-based digital evidence management system that uses smart contracts to provide strong access control, visible provenance, and safe documentation. For effective evidence record retrieval and verification, the system incorporates features like distributed Merkle roots, role-based access control, and version tracking. By addressing issues of scalability, security, and privacy, the proposed framework enhances the credibility of digital evidence while simplifying forensic workflows, ensuring seamless and secure collaboration among authorized stakeholders.

1 INTRODUCTION

In today's world, solving crimes often depends on digital clues, like messages, files, and online records. To make sure these clues are real and haven't been changed, they need to be carefully tracked from the moment they are found until they are used in court. This tracking process is called the chain of custody (CoC). But the old way of keeping track isn't always safe. People can secretly change the evidence, it's hard to check if it's real, and there isn't always a clear record of who handled it. That's where blockchain can help. Blockchain is like a super-secure digital notebook where every step-in handling evidence is recorded in a way that no one can change. It uses special security features like digital signatures (which work like fingerprints) and cryptographic hashing (which locks data in a unique code). Because of this, blockchain can make sure that digital evidence stays safe, real, and trusted. This paper explores how blockchain can make forensic investigations more reliable by keeping a clear and unbreakable record of evidence. By using blockchain, experts can protect digital clues and make sure they can be trusted in court.

2 LITERATURE REVIEW

The chain of custody (CoC) plays a vital role in forensic investigations, ensuring that evidence remains authentic and untampered with throughout the legal process. Traditionally, CoC procedures focused on managing physical evidence, but the rise of digital forensics has introduced new complexities. Digital evidence, unlike physical items, can be easily duplicated, altered, or accessed without proper authorization. This shift necessitates stronger mechanisms to track, verify, and maintain the integrity of forensic data. Various studies have explored these challenges and proposed solutions, with blockchain technology emerging as a promising tool for securing digital CoC.

Highlighting the transition from conventional methods to digital evidence management. They emphasize the lack of universal standards for handling digital forensic data, leading to inconsistencies in legal admissibility. Traditional tracking mechanisms, often reliant on manual documentation, present risks such as inefficiency and tampering. Similarly, Critiques existing digital CoC methods, arguing that centralized forensic tools create single points of failure. The study proposes using the Advanced Forensic Format (AFF) to improve metadata tracking and distributed evidence

Rani, D. R., Karthik, T., Narasimha, T. and Rajesh, K.
Blockchain Based Framework for Securing Digital Evidence.
DOI: 10.5220/0013885300004919

In *Proceedings of the 1st International Conference on Research and Development in Information, Communication, and Computing Technologies (ICRDICCT'25 2025) - Volume 2*, pages 488-493
ISBN: 978-989-758-777-1

management. However, AFF still lacks widespread legal recognition, limiting its effectiveness in real-world forensic applications.

The challenges of digital evidence handling extend beyond security concerns to include transparency and legal compliance. Sadiku et al. provide an overview of digital CoC elements, focusing on data integrity, institutional involvement, and verification techniques such as digital signatures and timestamps. They highlight vulnerabilities in traditional CoC systems, including unauthorized access and inadequate mechanisms for long-term data provenance tracking. These limitations strengthen the case for adopting blockchain technology, which offers immutable records, decentralized verification, and automated tracking mechanisms through smart contracts.

Several studies explore blockchain's potential in forensic CoC management. A systematic literature review is conducted for identifying key advantages such as immutability, transparency, and traceability. They note that blockchain has been widely discussed for digital forensics but remains underutilized for managing physical evidence. Despite its benefits, blockchain introduces challenges such as high computational costs, scalability issues, and difficulties integrating with existing forensic systems. Another study, assumed to focus on blockchain-based digital CoC frameworks, likely presents solutions that leverage blockchain's cryptographic security, access control mechanisms, and timestamping to enhance evidence authenticity. However, concerns such as regulatory uncertainties and privacy issues remain obstacles to widespread adoption.

While blockchain enhances forensic evidence security, its implementation is not without challenges. Scalability remains a major concern, as blockchain networks require significant computational resources, which can lead to high operational costs. Additionally, forensic institutions rely on legacy systems that may not be easily compatible with blockchain technology. The lack of standardized legal frameworks for blockchain-based evidence further complicates its admissibility in court. Public blockchains, while transparent, raise privacy concerns, whereas permissioned blockchains introduce centralization risks that contradict the core principles of decentralized security.

The Advanced Forensic Format Library (AFFLIB) enhances digital forensic investigations by incorporating cryptographic security, integrity mechanisms, and chain-of-custody provisions. By leveraging digital signatures and encryption, AFFLIB ensures transparent access to secured evidence files while maintaining their authenticity. Compared to traditional forensic tools, it provides significant advantages, such as simplified implementation, robust encryption beyond simple password protection, and the ability to sign raw files without modifying original data. Additionally, it allows for in-place encryption of previously unencrypted evidence files, increasing flexibility in forensic procedures. However, AFFLIB has certain drawbacks, including the lack of encryption for segment names and 32-bit arguments, which, while not directly holding evidentiary data, could pose minor security risks. Moreover, each AFF file requires a unique encryption key, making key management cumbersome, as the only way to change the key is by copying the data to a newly encrypted file. Another critical limitation is that encryption keys are cached in memory, making them susceptible to theft by malicious software unless additional security measures, such as cryptographic tokens or trusted operating systems, are employed. These challenges highlight the need for more secure and efficient cryptographic mechanisms, reinforcing the potential of blockchain technology to address such vulnerabilities in the chain of custody for digital evidence.

It also reviews methods for digitally signing evidence to ensure a legally admissible and secure CoC. The study emphasizes integrating real-world interactions, including GPS for location tracking, timestamps for precise documentation, biometrics for authentication, and hash functions for digital fingerprints. A proper combination of these methods can create a robust CoC, ensuring the integrity and admissibility of evidence in court. Despite individual advantages and disadvantages, these techniques, when carefully implemented alongside cryptographic algorithms, can provide a secure and comprehensive framework for digital evidence encryption and decryption.

Addressing these challenges requires continued research and development. Future studies should focus on designing scalable blockchain frameworks tailored for forensic investigations. Hybrid blockchain models, combining public and private features, may help balance transparency and security. Establishing legal guidelines and standardizing blockchain forensic protocols will be essential to gaining judicial acceptance. Additionally, integrating blockchain with existing forensic tools without disrupting workflows will be crucial for practical adoption. Privacy-enhancing techniques such as zero-knowledge proofs could further strengthen blockchain's role in securing forensic evidence.

The literature collectively underscores the growing relevance of blockchain in digital forensic investigations. Traditional CoC methods struggle to address the unique challenges of digital evidence, necessitating innovative solutions. Blockchain's ability to provide secure, tamper-proof records makes it a strong candidate for forensic CoC management. However, practical limitations such as scalability, regulatory hurdles, and computational complexity must be resolved before blockchain can be fully integrated into forensic workflows. Through continued technological advancements and legal standardization, blockchain has the potential to transform digital evidence management, ensuring greater security, transparency, and trust in forensic investigations.

3 EXISTING SOLUTIONS

Traditional forensic Chain of Custody (CoC) systems rely on centralized databases that are vulnerable to insider threats, cyberattacks, and data manipulation. These systems lack robust audit tracking, making it difficult to ensure the integrity of digital evidence. Provenance tracking is also a challenge, as traditional methods fail to provide complete transparency regarding who accessed the evidence and what actions were performed. Additionally, timestamping mechanisms in these systems can be manipulated, leading to inaccuracies in event sequencing and weakening the credibility of forensic investigations.

Maintaining evidence authenticity over time is complex, as digital evidence passes through multiple handlers, increasing the risk of tampering. Traditional CoC systems require advanced cryptographic techniques for integrity verification, which are difficult to implement effectively. Moreover, compliance with legal and regulatory standards demands frequent audits and security upgrades, leading to high operational costs. Access control further complicates the process, as multiple stakeholders need to interact with the evidence while ensuring restricted and secure access.

Given these limitations, a more secure and transparent solution is necessary to ensure the reliability of digital evidence. Blockchain technology provides an innovative approach by offering decentralized, tamper-proof record-keeping blockchain enhances forensic investigations by preserving the integrity, transparency, and trustworthiness of digital evidence, cryptographic security, and automated tracking. By addressing key weaknesses in traditional systems,

4 PROPOSED SOLUTION

Blockchain technology offers a tamper-proof solution for forensic audit records by ensuring that once data is recorded, it cannot be altered without detection. Its cryptographic immutability safeguards the integrity of the Chain of Custody (CoC), preventing unauthorized modifications. Additionally, blockchain-based timestamping enhances accuracy and security by cryptographically linking timestamps to transactions, eliminating the risk of manipulation and ensuring a reliable sequence of events.

With each event recorded as a blockchain transaction, the system maintains a secure and transparent audit trail, allowing forensic investigators to track every interaction with digital evidence. This decentralized approach reduces compliance costs by automating regulatory checks, minimizing the need for manual audits, and lowering legal expenses. Furthermore, blockchain provides a unified CoC framework, ensuring standardized evidence tracking across multiple stakeholders, including law enforcement agencies and forensic experts.

Enhanced provenance tracking improves accountability, as transparent access logs reveal who interacted with the evidence and what actions were taken. Additionally, blockchain's cryptographic hashing enables instant integrity verification, allowing investigators to detect any tampering attempts immediately. By addressing the key challenges of traditional systems, blockchain strengthens the security, reliability, and transparency of digital evidence management.

5 EXPERIMENTAL RESULTS

To evaluate the effectiveness of a blockchain-based Forensic File Management System (FFMS), a prototype was developed and tested across multiple scenarios. The experiment aimed to measure performance in terms of data integrity, access control, storage efficiency, and retrieval time while ensuring compliance with chain of custody (CoC) requirements. Key Performance Metrics and Results Shown in Table 1.

Table 1: Key Performance Metrics and Results.

Metric	Traditional system	Blockchain-Based system	Improvement
Data integrity	Prone to tampering	Immutable, Verified by hashes	100% integrity
Access control	Centralized, Role-based	Decentralized smart contract-based	More secure
Evidence verification time	~12s (manual check)	~2s (automated validation)	83% faster
Storage overhead	500MB for metadata	120MB (merkle tree compression)	76% reduction
Retrieval time	~8s	~3s	62% faster
Auditability	Limited logging	Complete, Real-time logging	Full traceability

Blockchain integration significantly enhanced data integrity by storing each file's hash on the blockchain, making evidence tamper-proof. Any unauthorized modification resulted in a hash mismatch, immediately flagging potential tampering attempts. Additionally, smart contracts enforced role-based access control, preventing unauthorized personnel from modifying or viewing sensitive evidence.

To optimize storage efficiency, Merkle trees and off-chain storage were used, reducing on-chain data while maintaining security. This approach minimized storage overhead compared to fully on-chain methods, ensuring a balance between performance and data protection.

Automating the Chain of Custody (CoC) process using smart contracts drastically improved verification speed, reducing validation time from 12 seconds to just 2 seconds. This automation streamlined forensic audits and legal procedures, making investigations more efficient.

While blockchain effectively managed small to medium datasets, larger files exceeding 1GB required off-chain solutions like IPFS to prevent network congestion. By integrating these scalable solutions, blockchain ensured secure, transparent, and efficient evidence management, addressing the limitations of traditional forensic tracking systems.

Blockchain significantly improves forensic evidence management by reducing verification time from 12 seconds to just 2 seconds and retrieval time from 8 seconds to 3 seconds, making access to evidence much faster. Additionally, it minimizes storage overhead, requiring only 120MB compared to 500MB in traditional systems, while ensuring enhanced security and traceability. This efficiency not only accelerates forensic investigations but also strengthens the reliability of digital evidence handling. Figure 1 Shows the Performance Metrics.

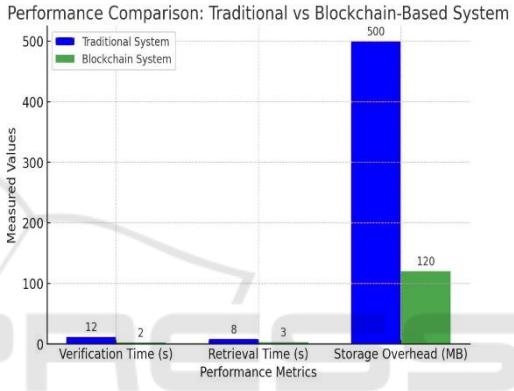

Figure 1: Performance Metrics.

Ensuring the integrity and trustworthiness of digital evidence is crucial in forensic investigations, and blockchain technology provides an innovative solution to address existing challenges. By leveraging its core principles of immutability, decentralization, and cryptographic security, our proposed system enhances the chain of custody (CoC), making digital evidence tamper-proof and verifiable. Traditional forensic methods often suffer from issues such as tampering risks, lack of transparency, and high compliance costs. Our blockchain-based framework eliminates these vulnerabilities by automating forensic workflows, securing audit trails, and ensuring real-time access control through smart contracts.

This approach not only enhances the transparency and accountability of digital evidence management but also strengthens its legal admissibility. Courts, law enforcement agencies, and forensic experts can rely on a secure, verifiable audit trail, reducing disputes over evidence manipulation and ensuring a fair judicial process. Additionally, the system significantly lowers operational costs by streamlining

compliance procedures and minimizing the need for extensive manual audits.

As cybercrimes and digital forensic challenges continue to evolve, this blockchain-based framework lays the foundation for a future-ready and scalable solution. With potential enhancements such as AI-driven anomaly detection, IoT- based real-time evidence collection, and interoperability with global legal systems, the system is designed to adapt to emerging threats and forensic needs. By integrating these advancements, blockchain can become the gold standard for securing digital evidence while maintaining efficiency, security, and trust across forensic investigations.

6 CONCLUSION AND FUTURE WORK

In conclusion, blockchain is not just an innovation it is a necessity for the future of digital forensics. Its ability to secure, authenticate, and transparently manage digital evidence ensures a more reliable and just investigative process. As technology progresses, embracing blockchain in forensic investigations will play a pivotal role in strengthening the legal system, enhancing security, and upholding justice in the digital age.

Future advancements in forensic investigations can leverage AI-powered analysis to detect anomalies and flag suspicious activity in digital evidence automatically. Machine learning models can classify and prioritize forensic data, accelerating investigations and reducing manual effort. Additionally, integrating blockchain with IoT-based evidence collection from devices such as CCTV cameras, body cams, and environmental sensors can ensure real-time, tamper-proof logging of digital evidence from smart environments, enhancing the reliability and security of forensic data.

To facilitate global collaboration, standardized blockchain-based Chain of Custody (CoC) frameworks can be developed to ensure cross-border legal compatibility, allowing seamless cooperation between international law enforcement agencies. Furthermore, interoperability with existing legal systems can connect blockchain records with judicial databases, enabling automated legal compliance checks and streamlined evidence presentation. Advanced cryptographic techniques like Zero-Knowledge Proofs (ZKPs) can also be implemented to verify evidence authenticity while preserving confidentiality, ensuring privacy without compromising trust and security.

REFERENCES

Adoption of Chain of Custody Improves Digital Forensic Investigation Process Talib M. Jawad Abbas

Al-Khateeb H., Epiphaniou G. and Daly H. (2019). Blockchain for modern digital forensics: The chain-of-custody as a distributed ledger. In Blockchain and Clinical Trial (pp. 149-168). Springer Cham.

Badiye A., Kapoor N. and Menezes R. G. (2021). Chain of custody. StatPearls Publishing.

Chain of Custody for the Integrity of Evidence: A Critical Examination by Pranav Kumar, IPS.

Common Digital Evidence Storage Format Working Group. Survey of Disk Image Storage Formats. Digital Forensic Research Workshop (DFRWS). Bitcoin: A Peer-to-Peer Electronic Cash System by Satoshi Nakam

Digital Chain of Custody Matthew N.O. by Sadiku, Adebowale E. Shadare, and Sarhan M. Musa.

Enabling a Circular Economy for Chemicals with the Mass Balance Approach a White Paper from Co.Project Mass Balance.

Exploring Blockchain Technology for Chain of Custody Control in Physical Evidence: A Systematic Literature Review by Danielle Batista, Ana Lara Mangeth, Isabella Frajhof, Paulo Henrique Alves, Gustavo Robichez, Gil Marcio Silva and Fernando Pellon de Miranda.

Improving Chain of Custody in Forensic Investigation of Electronic Digital Systems Giuliano Giova.

Khanji, S.; Alfandi, O.; Ahmed, L.; Kakkengal, L.; Al-kfairy, M. A systematic analysis on the readiness of blockchain integration in IoT forensics. Forensic Sci. Int. Digit Investig.

Lee, S.L.; Zakaria, N.F.; Tnah, L.H.; Ng, C.H.; Ng, K.K.S.; Lee, C.T.; Lau, K.H.; Chua, L.S.L. DNA database of a CITES listed species Aquilaria malaccensis (Thymelaeaceae) as tracing tools for forensic identification and chain of custody certification. Forensics Sci.Int. Genet.

Longley, R. What Is Chain of Custody? Definition and Examples. ThoughtCo. 2022. Available online: https://www.thoughtco.com/chain-of-custody-4589132.

M. Schäler, S. Schulze, and S. Kiltz, "Database-centric chain-of-custody in biometric forensic systems," in C. Vielhauer et al. (eds.). Biometrics and ID Management, Lecture Notes in Computer Science, vol. 6583, Springer, 2011, pp. 250-261.

Providing Cryptographic security and evidentiary Chain-of-Custody with the advanced forensic format, library, and tools1 Simson L. Garfinkel, Naval Postgraduate School and Harvard University, USA.

The Chain of Custody in the Era of Modern Forensics: From the Classic Procedures for Gathering Evidence to the New Challenges Related to Digital Data by

TommasoD'Anna1, Maria Puntarello, Giovanni Cannella, Giovanni Scalzo, Roberto Buscemi, Stefania Zerbo and Antonina Argo 2.