Digital Forensic Evidence Integrity Through Blockchain Technology

Sadhana R

Department of CSE [Cybersecurity and Blockchain Technology] [Sastra Deemed University]

Abstract—**With the rise of cybercrime, the integrity and security of digital evidence have become more critical than ever. Investigations increasingly rely on ensuring that the collected evidence is legally valid, tamper-proof, and presented with an unbroken chain of custody (CoC). The CoC refers to a complete, documented history of who collected, transferred, stored, and presented the evidence. Traditional CoC methods, often recorded on paper or spreadsheets, are vulnerable to human error, manipulation, and lack of transparency. This paper proposes a blockchain-based approach to ensure the integrity and traceability of digital forensic evidence. Each action—collection, transfer, storage, and access—is recorded as an immutable, timestamped transaction on a distributed ledger. Blockchain technology provides transparency, tamper-resistance, and auditability, making it a trustworthy solution for modern forensic investigations.**

***Index Terms*—Blockchain, Chain of Custody, Cybercrime, Digital Forensics, Evidence Integrity**

1. INTRODUCTION

Cyber crimes have seen a significant surge globally, with financial fraud, ransomware attacks, and data breaches being the most prevalent types. These crimes often involve digital evidence such as emails, logs, images, videos, and application data. Digital forensics plays a vital role in identifying, preserving, analyzing, and presenting such electronic evidence in a legally admissible manner. Chain of Custody (CoC) is crucial in digital forensics. It refers to a full, unbroken record of who collected, transferred, stored, and presented the evidence. Traditional CoC methods are often paper-based and susceptible to manipulation or misplacement. This paper proposes using blockchain technology to secure the CoC, enhancing trust in the integrity of digital forensic evidence.

2. RELATED WORK

Several studies have explored blockchain for improving digital forensic evidence integrity. ARES Conference (2020) proposed a permissioned Ethereum blockchain for logging custody events but lacked multi-agency handling features. Bonomi et al. (2018) introduced B-CoC using Ethereum to automate metadata logging, though it lacked role-based access control. Shahaab et al. (2021) proposed "EvidenceChain" for high-corruption environments, but it remained conceptual without implementation. This paper builds on these approaches by proposing a simplified, auditable blockchain model focused on digital evidence handling in cybercrime cases.

3. PROPOSED SYSTEM / METHODOLOGY

The proposed system uses a permissioned blockchain to record every event associated with evidence handling. It involves four main components: Evidence Collector App, Blockchain Ledger, Smart Contract Engine, and Digital Identity System. Each evidence action (collection, transfer, access) is hashed and stored on the blockchain. Only authorized personnel can perform actions via smart contracts. This ensures immutability, transparency, and legal defensibility.

4. SIMULATION / PROTOTYPE

A simulation was developed using Python. Each event is hashed and added to a blockchain structure. The hash chain validates that any modification breaks the integrity. This demonstrates how blockchain ensures tamper-proof records and auditability in real time.

5. RESULTS AND DISCUSSION

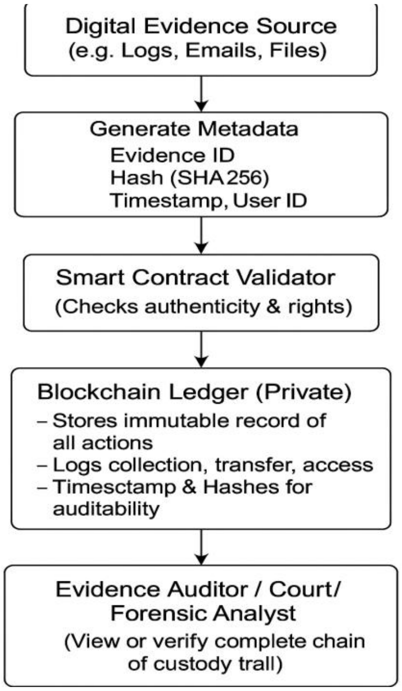
The simulation showed that blockchain-based logging ensures transparency and traceability. Compared to traditional CoC (manual logs), blockchain provides stronger audit trails and trustworthiness. Tampering attempts are easily detectable due to hash chaining. Legal authorities can access a complete, unchangeable record of evidence handling.

6. CONCLUSION AND FUTURE WORK

This paper proposed a blockchain-based approach for securing the chain of custody in digital forensics. The simulation confirmed improved transparency, traceability, and tamper-resistance. Future work may include integrating real forensic tools, legal compliance testing, and deploying a smart contract-based permissioned blockchain in live investigation environments.

7. SYSTEM ARCHITECTURE DIAGRAM

The following diagram illustrates the architecture of the proposed blockchain-based chain of custody system for digital forensic evidence. It shows how digital evidence is collected, verified, stored on the blockchain, and audited for legal use.


Digital Evidence Source
(e.g. Logs, Emails, Files)
Generate Metadata
Evidence ID
Hash (SHA256)
Timestamp, User ID
Smart Contract Validator
(Checks authenticity & rights)
Blockchain Ledger (Private)
– Stores immutable record of all actions
– Logs collection, transfer, access
– Timesctamp & Hashes for auditability
Evidence Auditor / Court/ Forensic Analyst
(View or verify complete chain of custody trall)

REFERENCES

[1] Bonomi, S., Caselli, M., & Cerroni, W. (2018). B-CoC: A Blockchain-Based Chain of Custody for Evidence Management in Digital Forensics. In Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES '18).

[2] Shahaab, A., Lyle, J., & Buchanan, W. J. (2021). EvidenceChain: A Blockchain-Based Forensic Chain of Custody for Evidence Management in High-Corruption Environments. Journal of Information Security and Applications.

[3] ARES Conference. (2020). Blockchain-Based Digital Evidence Handling: Smart Locks and Custody Event Logging. Proceedings of the International Conference on Availability, Reliability and Security.