myresearchgo Volume 1, November Issue 8, 2025, ISSN: 3107-3816 (Online)

Blockchain for Tamper-Proof Digital Evidence Logging and Chain of Custody in Cybercrime Investigations

Shalini kumari
Shalinidas281@gmail.com
G.H raisoni college of Engineering and managment

Pravin kulurkar
pravin.kulurkar@raisoni.net
G.H raisoni college of Engineering and management

Priti bihade
priti.bihade@ghrua.edu.in
G.H raisoni college of Engineering and management

1. Introduction

In this modern age of technology, crime no longer only exists in the physical domain. Cybercrimes like hacking, data breaches, identity theft, and internet fraud have become prevalent. Solving such crimes involves dealing with digital evidence like emails, log files, metadata, images, or internet transactions which must be kept authentic, traceable, and tamper-proof throughout the investigation process.

Nevertheless, it is a big challenge to ensure integrity of digital evidence. Legacy systems tend to be based on centralized databases and manual record-keeping, hence they are prone to tampering, unauthorized viewing, or accidental alteration. As soon as the authenticity of evidence is doubted, the entire case is doomed in court.

To address these issues, blockchain technology presents a viable solution. Its potential to produce an immutable, transparent, and verifiable ledger is best suited for capturing digital evidence and preserving a secure chain of custody in the investigation of cybercrimes.

2. Understanding Digital Evidence and Chain of Custody

Digital evidence is any data stored or communicated in digital format that can be utilized in court. It may include emails, mobile data, video surveillance, documents, or network logs. Since digital data can be easily copied, manipulated, or deleted, the chain of custody — a paper trail indicating who gathered, stored, transferred, analyzed, and stored the evidence at each point — must be established.

A legitimate chain of custody guarantees:

- The testimony given in court is real and not tampered with.
- Each person who handled the evidence is identified and accountable.
- There is absolute openness from the moment the evidence is gathered to the moment it is brought forward in court.

Sadly, conventional approaches using manual logs, spreadsheets, or centralized servers are prone to error and susceptible to tampering. This is where the blockchain comes in to revolutionize the process.

3. What is Blockchain?

Blockchain is the most impactful technology of the 21st century. It was initially created to facilitate digital currency such as Bitcoin, and today it has become a core technology for numerous industries like finance, healthcare, supply chain, cyber security, and government systems.

In essence, blockchain is a digital, decentralized, distributed ledger that stores transactions or information on a network of computers in a secure, transparent, and tamper-evident fashion. Blockchain does not use a central authority like traditional databases but instead uses a network of participants (nodes) that all agree on validating and storing information.

Step-by-Step Process: How Blockchain Works

Step 1: Transaction Creation

A user creates a transaction.

Example: Alice transfers 2 digital coins to Bob.

- This transaction includes fundamental information:
- Sender and recipient digital addresses
- Amount transferred
- Digital signature for authentication

This transaction is sent to the blockchain network (collection of computers known as nodes).

Step 2: Transaction Verification

All network members should check before they accept a transaction that it's valid.

Verification ensures:

- The sender possesses sufficient balance or permission to perform the transaction.
- The transaction information (digital signatures, timestamps, etc.) is genuine.

Step 3: Clustering into a Block

After verification, several legitimate transactions are clustered together to create a block.

For instance:

If there are 1,000 legitimate transactions within a specific time window, they are clumped into a single block.

The block contains:

- A special block ID
- All transaction data
- A timestamp
- The hash of the last block

A nonce (random number for mining)

Step 4: Hashing (Digital Fingerprint Creation)

Data from each block is fed into a cryptographic hash function — a mathematical formula that maps input data of variable length to a fixed-length string (e.g., 64 characters).

For instance:

Input: "Hello World"

Output Hash:a591a6d40bf420404a011733cfb7b190d62c65bf0bcda32b57b277d9ad9f146e

If one letter changes even slightly, the hash completely changes — making it easy to detect tampering.

The hash is a digital fingerprint of that block.

Step 5: Consensus Mechanism (Nodes' Agreement)

Now that the block is prepared, it has to be validated by the network before it can be added to the chain.

This is achieved via a consensus mechanism, whereby all nodes come to a consensus on the same version of truth.

Typical Consensus Mechanisms:

Proof of Work (PoW)

- Used in Bitcoin.
- Miners race to find a complicated math puzzle through computational effort.
- The winner does the validation of the block and is rewarded.
- Extremely secure but power-hungry.

Proof of Stake (PoS)

- Implemented in Ethereum 2.0 and subsequent systems.
- Validators are selected in proportion to the cryptocurrency they possess ("stake").
- Faster and more efficient than PoW.

Practical Byzantine Fault Tolerance (PBFT)

- Applicable for private blockchains.
- Nodes discuss and vote to determine valid transactions.
- After consensus is reached, the block is ready for inclusion.

Step 6: Block Addition to the Chain

Once validated successfully, the block gets added to the blockchain.

It points to the hash of the last block, which is what reliably connects it to the chain.

Example:

1.Block #1 → Genesis block (the initial one)

2.Block #2 → Holds the hash of Block #1

3.Block #3 → Holds the hash of Block #2

If someone attempts to modify Block #2, its hash is different — and Block #3's link is broken.

This reveals any attempt at tampering right away.

Step 7: Distribution and Synchronization

- After being added, the new block is propagated through all nodes in the network.
- Every node gets its copy of the blockchain updated with the new block.
- Since all nodes contain a full copy of the ledger, it is virtually impossible for the hacker to modify all copies at once.
- This decentralized mechanism is what makes blockchain so secure and reliable.

Step 8: Immutability and Transparency

From here onwards, the information in the block is immutable — it can neither be altered nor destroyed.

If an individual tries to alter an earlier record:

- The hash of the block is altered.
- The discrepancy jeopardizes the chain.
- Other nodes refuse the tampered record.

Blockchain, therefore, guarantees:

- Transparency: All network participants can view transactions.
- Integrity: Records are consistent and reliable.
- Security: Cryptography prevents data from being modified without authorization.

Example of How Blockchain Works (Simple Scenario)

Let's consider a real-world example of three users: Alice, Bob, and Carol.

- Alice initiates a transfer of 5 digital coins to Bob.
- The transaction request is propagated to every node in the network.
- Every node verifies Alice's balance to see if she has a minimum of 5 coins.

- Once authorized, the transaction is combined with others in a block.
- The block is verified via the consensus mechanism.
- The block is appended to the blockchain.
- Each node updates the copy of its ledger to indicate the new transaction.

Result: Bob gets paid 5 coins, and this record is now tamper-proof and permanent.

4. Role of Blockchain in Cybercrime Investigations

Blockchain technology may be employed in the handling of digital evidence in the course of cybercrime investigations to securely log, monitor, and confirm all actions involving digital evidence handling. Every time evidence is acquired, analyzed, or moved, a related entry on the blockchain is created. The entry contains metadata like:

- Evidence ID
- Name and digital signature of the collector
- Time and date of collection
- Location
- Hash of the digital file
- Later transfers or analyses

Each transaction is encrypted and referenced to the last one, forming a chronological, un-tamperable path that is an authoritative chain of custody.

5. Blockchain Based Chain of Custody System

A chain of custody system based on blockchain can be imagined in these steps:

Evidence Collection: As investigators gather digital evidence, its hash value (digital fingerprint) is calculated. The hash, with metadata (date, time, location, officer ID), is entered into the blockchain.

Evidence Transfer: When evidence is transferred to another investigator or lab, the transfer information is included as an additional blockchain transaction, maintaining complete traceability.

Evidence Analysis: When examined forensically, the system keeps a record of what accessed the evidence, when, and what was done. Any change to the information is easily traceable because the hash would no longer agree with the original entry.

Court Presentation: In court, investigators can prove that the evidence was left unchanged by using the blockchain record, which displays all actions taken from the time it was collected.

This is an automated, verifiable mechanism that provides transparency, trust, and admissibility of digital evidence.

6. Advantages of Using Blockchain

In cybercrime cases, integrity and authenticity of digital evidence need to be maintained. Anything that alters, loses, or tampers with evidence can make it inadmissible in court and jeopardize the prosecution altogether.

Traditional digital evidence management systems are based on centralized databases and human records, which can be tampered with, accessed without authorization, and deleted accidentally. Blockchain technology offers a secure, efficient, and transparent solution for such problems.

By leveraging blockchain technology, investigators can create an indelible digital evidence management system that has a verifiable and auditable chain of custody from evidence collection through court presentation.

✧ **Tamper-Proof and Immutable Records**

A primary advantage of the blockchain is that it is immutable once data is written to the blockchain it cannot be altered or deleted without consensus by the network.

- Each piece of digital evidence can be assigned a unique cryptographic hash value, an electronic fingerprint of sorts.
- Once the evidence is placed on the blockchain, its hash and metadata (date, time, collector ID, location) are secured forever.
- If someone tried tampering with the evidence at some future time, even the smallest change will create a new hash, immediately revealing tampering.
- This feature guarantees that digital evidence is tamper-proof and authentic, and robust integrity protection is guaranteed throughout the investigation.

✧ **Transparent and Verifiable Chain of Custody**

A chain of custody is a record which traces handling of the evidence from the moment it is seized until the moment it appears in court. Blockchain technology can make the process secure and automate the same through transparent history of transactions.

Everything done with the evidence such as movement, transfer, analysis, or storage is recorded on the blockchain as a time-stamped transaction. This provides:

- Complete and verifiable history of who handled or moved the evidence
- Date and time for every operation
- Digital signatures to confirm each player's identity
- Because all records are time-stamped and viewable to authorized users, blockchain avoids evidence handling disputes in court.
- Stronger Security by Cryptography
- Blockchain employs advanced cryptographic functions to protect data within it.
- Each transaction is hashed and cross-referenced to the preceding transaction using hash functions and public-private key encryption.
- Investigators or forensic officers utilize private keys to sign and verify entries of evidence.
- Adding or reading records can only be done by authorized personnel, reducing the opportunity for insider manipulation or illegal access.

This cryptographic system ensures that even if a single node or database is attacked, the entire blockchain remains safe and secure.

✧ **Decentralization and Elimination of Single Points of Failure**

Traditional digital evidence systems rely on centralized databases, which are vulnerable to hacking, data loss, or corruption.

In contrast, blockchain works on a decentralized peer-to-peer network. Each node on the network maintains a complete copy of the blockchain ledger, making it effectively impossible for an attacker to alter all copies simultaneously.

This decentralization provides:

- **High availability:** The system remains operational even if one or more nodes fail.
- **Resilience:** Recovery of data is easier because of the existence of multiple copies of the ledger.
- **Trustworthiness:** No single authority can manipulate or delete evidence records.

Thus, blockchain ensures that digital evidence remains secure and accessible even in the face of cyberattacks or system failures.

✧ **Automation with Smart Contracts**

Smart contracts are self-executing programs stored on the blockchain that automatically perform actions when certain conditions are met.

In digital forensics, smart contracts can automate several tasks, such as:

- Automatically recording when evidence is collected, transferred, or analyzed
- Sending alerts when unauthorized access attempts occur
- Triggering audit logs or approval requests

This automation reduces human error, ensures consistent procedures, and enhances the reliability of the **chain of custody** documentation.

✧ **Improved Trust and Legal Admissibility**

In court, the credibility of evidence often depends on the ability to prove that it has not been tampered with.

Because blockchain provides an **immutable, transparent, and time-stamped record**, it strengthens the **legal admissibility** of digital evidence.

- Judges and attorneys can verify the integrity of evidence independently.
- The blockchain ledger serves as an **independent, verifiable proof** of authenticity.
- Investigators gain credibility by demonstrating secure evidence management practices.

This increases overall **trust** in digital investigations and strengthens the judicial process.

✧ **Real-Time Monitoring and Auditability**

Blockchain allows **real-time tracking** of evidence status. Investigators and authorized agencies can monitor:

- When and where evidence was accessed
- Who handled it last
- How long it remained in a specific phase of custody

Every action is permanently recorded, enabling instant audits and compliance checks.
This continuous monitoring capability makes blockchain ideal for agencies dealing with large volumes of digital evidence, such as cybersecurity teams and forensic labs.

✧ **Interagency Collaboration and Data Sharing**

In many cybercrime cases, multiple organizations—such as police, forensic labs, and judicial departments—need to access or verify evidence.

Blockchain facilitates **secure data sharing** through controlled permissions and cryptographic access.

- Different agencies can access the same blockchain ledger without compromising confidentiality.
- Each participant's actions are logged, maintaining accountability.
- Data remains synchronized and consistent across all organizations.

This promotes **collaboration, efficiency, and trust** among agencies handling complex cybercrime cases.

✧ **Reduction of Administrative Burden**

Traditional evidence management involves extensive paperwork, manual recordkeeping, and repetitive verification steps.

Blockchain simplifies this through:

- **Automatic digital logging** instead of manual entry
- **Instant verification** of data authenticity via hash comparison
- **Elimination of intermediaries**, reducing delays and administrative workload

This not only saves time but also minimizes the chance of human error and procedural lapses in evidence handling.

✧ **Resistance to Insider Threats**

One of the most overlooked vulnerabilities in digital forensics is the **insider threat**—when authorized personnel intentionally or unintentionally alter data.

Since blockchain records every action immutably and transparently:

- Any unauthorized change becomes immediately visible.
- All activities are linked to verified digital signatures, making it easy to trace responsible individuals.
- Attempts to manipulate evidence can be detected and prevented early.

This deters internal misuse and enhances accountability across the entire evidence-handling process.

✧ **Long-Term Preservation and Integrity**

Digital investigations may span years before they reach conclusion in court. During that time, evidence must remain **intact, accessible, and verifiable**.

Blockchain provides a **durable and permanent storage solution**:

- Time-stamped records remain immutable even after decades.
- Each block's link to previous blocks ensures a full historical record.
- Cloud or distributed storage integration ensures availability and redundancy.

This guarantees the **long-term preservation** of digital evidence and ensures its **forensic reliability** during future audits or retrials.

✧ **Increased Public and Institutional Confidence**

The transparency and reliability of blockchain-based systems promote public confidence in digital investigations.
Citizens, courts, and institutions can trust that:

- Evidence is collected and stored ethically.
- No tampering or bias influences the results.
- Every procedural step can be independently verified.

This contributes to stronger justice delivery, improved cooperation between law enforcement and the public, and higher confidence in digital legal processes.

7. Integration with Digital Forensics Tools

Blockchain can be integrated with the digital forensics tools for automated logging of actions. For instance:

- This means that if a forensic tool extracts data from a suspect's device, it will automatically record the operation details in the blockchain.
- Any hash mismatch during verification will raise the alarm for possible tampering.

The access permissions are actually managed through cryptographic keys so that only the authorized users can add or view records.

8. Case Example(Conceptual)

Imagine a cybercrime case involving unauthorized access to a company's server. Investigators collect hard drives, emails, and network logs as digital evidence.

- Each piece of evidence is assigned a unique ID and hashed.
- Hash values and investigator details are logged on a private blockchain shared among law enforcement, forensic labs, and prosecutors.
- As evidence moves through various stages from collection to analysis to court presentation each transaction is recorded transparently.
- The court can verify that the evidence's digital fingerprint remains identical to the original, proving it has not been altered.

Such a system minimizes disputes over evidence authenticity and strengthens the prosecution's case.

9. Challenges and Limitations

Despite its advantages, several challenges must be addressed:

- **Scalability:** As evidence logs increase, the blockchain may become large and slow.
- **Privacy Concerns:** Sensitive data must be encrypted to prevent unauthorized disclosure.
- **Interoperability:** Integration with existing law enforcement databases and forensic systems requires standardization.
- **Legal Acceptance:** Courts and law enforcement agencies must legally recognize blockchain-based records as valid evidence.
- **Technical Expertise:** Investigators and legal professionals need training to use blockchain systems effectively.

10. Future Directions

The future of blockchain in cybercrime investigations looks promising. Possible advancements include:

- **Hybrid Blockchain Systems:** Combining public and private blockchains for better scalability and control.
- **AI Integration:** Using artificial intelligence to detect anomalies or tampering patterns in blockchain logs.
- **Global Standards:** Developing international frameworks for blockchain-based evidence management.
- **Judicial Acceptance:** Legal systems worldwide are slowly adapting to accept blockchain-based evidence records.

As technology evolves, blockchain could become the foundation for digital trust and accountability in all forms of criminal investigations.

11. Conclusion

Maintaining the integrity and authenticity of digital evidence is critical in cybercrime investigations. Traditional methods often fail to guarantee a secure and transparent chain of custody. Blockchain

technology with its immutable, decentralized, and transparent features offers a revolutionary solution.

By recording every evidence-related transaction on a tamper-proof ledger, blockchain ensures that digital evidence remains trustworthy, admissible, and verifiable throughout the investigation and trial process. While challenges remain, its adoption could transform the future of digital forensics, law enforcement, and judicial transparency.

Abbreviations

DLT: Distributed Ledger Technology

ID: Identification

AI: Artificial Intelligence

IT: Information Technology

References

1. Kshetri, N. (2021). *Blockchain and the Economics of Digital Evidence.* Journal of Cybersecurity.
2. Liu, Y., & Zhao, J. (2020). *Blockchain for Digital Forensics and Evidence Management.* IEEE Access.
3. Alenezi, M., & Abuaddous, H. (2023). *Chain of Custody Using Blockchain in Cybercrime Investigations.* International Journal of Computer Science and Information Security.
4. National Institute of Standards and Technology (NIST). (2022). *Guidelines on Digital Evidence Handling*
5. A Blockchain-Based Chain of Custody for Evidences Management in Digital Forensics (Bonomi, Casini & Ciccotelli, 2018/2019)
6. Bonomi, S., Casini, M., & Ciccotelli, C. (2019). *B-CoC: A Blockchain-Based Chain of Custody for Evidences Management in Digital Forensics.*
7. In International Conference on Blockchain Economics, Security and Protocols (Tokenomics 2019). DOI:10.4230/OASIcs.Tokenomics.2019.12.
8. Miller, A., & Singh, A. (2019). *Chain of Custody and Evidence Integrity Verification Using Blockchain Technology*. International Conference on Cyber Warfare & Security. DOI:10.34190/iccws.19.1.2025.
9. *Potential applicability of blockchain technology in the maintenance of chain of custody in forensic casework.* Egyptian Journal of Forensic Sciences, 14, 12. (2024). (2022?) *Management of the Chain of Custody of Digital Evidence Using Blockchain and Self-Sovereign Identities.* IEEE Access.
10. *Digital Evidence Security System Design Using Blockchain Technology*. IIETA IJSSE.
11. Akbarfam, A. J., Heidaripour, M., Maleki, H., Dorai, G., & Agrawal, G. (2023). *ForensiBlock: A Provenance-Driven Blockchain Framework for Data Forensics and Auditability.* arXiv.