WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Survey on Blockchain in Digital Forensic

Laxmi Mullatti [a], Swati Hattiholi [b], Dr. Pijush Barthakur [a,b,*]

Student, MCA, KLS Gogte Institute of Technology College Belgaum-590008, India [a]
Student, MCA, KLS Gogte Institute of Technology College Belgaum-590008, India [b]

A B S T R A C T

In today's world, there is a growing concern about how to tackle the continuously expanding problem of cybercrime. In response, law enforcement officials and security firms use sophisticated digital forensics techniques to analyse and investigate cybercrimes effectively. The use of Blockchain technology is reshaping the landscape of digital investigations by ensuring the security and trustworthiness of digital evidence. This paper examines how incorporating blockchain into digital forensics enhances the reliability of evidence.

Blockchain ensures the safety of evidence by preventing changes and recording every alteration. This strengthens the reliability of evidence during investigations and in court proceedings. However, employing blockchain in investigations presents challenges, such as the need for faster functionality and expertise in its utilization.

As blockchain technology improves collaborative efforts will enhance the effectiveness of investigations and ensure the safety of digital evidence.[1]

1.INTRODUCTION

When solving crimes using digital evidence a significant challenge is the proper management of that evidence. Digital proof such as information from phones or computers, plays a crucial role in linking individuals to criminal activities. Ensuring the safety and trustworthiness of this evidence is paramount as it transitions from initial investigators to higher authorities who handle cybercrime cases.

However, it's challenging due to the risk of tampering or errors in tracking it all.

There's this fascinating concept called blockchain, initially developed for Bitcoin which could offer assistance. It operates as an exceptionally secure digital ledger composed of interconnected blocks of information. As more details are added, it continually expands. Each block contains transaction data and is linked to the preceding one. This technology has the potential to revolutionize the preservation of digital evidence, ensuring its safety and reliability.

In digital records, each component is accompanied by a timestamp and a link to its preceding element, ensuring seamless connectivity. Blockchain, incorporating records of transactions, cryptographic codes, agreements, and regulations, is undergoing enhancements by a team known as Hyperledger. Chain of Custody (CoC), utilized as legal proof, must demonstrate its unaltered status during investigations. It is crucial to maintain the integrity of evidence from discovery to courtroom presentation. Thus, CoC handling should adhere to standard evidence management protocols. Key considerations for CoC include verifying authenticity, tracking from inception to conclusion, monitoring interactions, ensuring accuracy, and safeguarding integrity. Utilizing these measures entails devising a comprehensive plan to optimize CoC functionality, including a secure private record and an intelligent framework for tracking evidence custody.[2]

2.Existing COC and B-COC

The chain of custody is the process of controlling and maintaining digital evidence collected from its initial stage until it is presented in court. In the existing system, evidence is passed through several higher authorities by lower authorities, and there are chances of this evidence being tampered with before it reaches the court.

The B-COC, which is a Blockchain-based chain of custody, provides a proper solution to this problem. By using features of Blockchain such as immutability, distributed ledger, and consensus, we can maintain the chain of custody in a more secure and tamper-proof way.

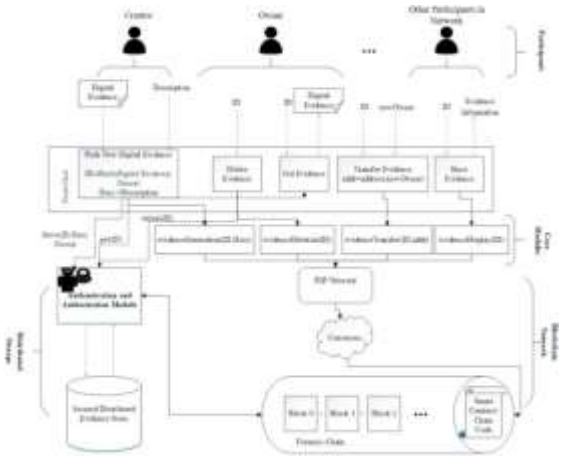

Fig: Operational flow of forensic chain

[Ref:https://ars.elscdn.com/content/image/1-s2.0-S174228761830344X-gr6.jpg]

The originality of the evidence is preserved as it is stored with all the participants in the network. The evidence itself is not passed as data in the chain; rather, a hash value is passed. The hash is computed using Base64, a binary-to-text encoding algorithm. The image of the evidence is stored locally and processed to generate a textual format using the Base64 algorithm. The image is first converted into a bitmap of pixels and then into a stream of bytes. The image is then written to the disk in a series of byte formats. When we run the Base64 algorithm, it reads the bytes from the disk, groups them into blocks of 6 bits each, and replaces them with 64 place value.

3.MAINTAINING CHAIN OF CUSTODY

A. Lifecycle of Digital Evidence

The process of documenting evidence and maintaining it is usually termed the chain of custody. Detailed information about the persons involved in the investigation process is stored. The chain of custody starts with the collection of evidence from the crime scene. Then the evidence is passed to the investigation cell. The evidence collected by the first responder is passed to the immediate forensic investigator for further analysis. The evidence is then transferred to the prosecutor, the lawyer who conducts the case against a defendant in a criminal court. The analyzed data is then transferred to the defense, which may attempt to challenge the criminal charges. Finally, the evidence is transferred to the court.

B. Security Issues in Chain of Custody

Digital evidence is an integral part of the investigation process. Therefore, in the judicial process, evidence also plays an important role. The problem encountered these days is the security gap in handling this evidence. The main problem in the chain of custody is the documentation and recording of interactions with the evidence. When evidence is used by multiple parties there is a risk of tampering. In a court of law, detailed information is needed to support the investigation process, so it becomes very important to keep an accurate log. One of the major challenges in the chain of custody is maintaining the integrity of the data. The integrity of digital evidence ensures that the evidence is complete and not tampered with. It is crucial to ensure that parties interacting with and making changes to the evidence are authorized.

C. Digital Evidence Framework

In the existing system, the court of law does not consider digital evidence to be reliable unless there is evidence of empirical testing regarding the techniques involved in its production. Documentation, i.e., paperwork, is maintained to identify the various aspects of digital evidence.

When the evidence is transferred from one entity to another, all the details regarding the entity as well as the evidence are documented on a sheet. The document is later attached to the charge-sheet generated during the investigation. However, there is no standard approach currently being followed to acquire evidence and trace the current owner of digital evidence. A standard process for data acquisition and tracing of the current owner would help the court of law determine the reliability of digital evidence.

D. Ingenuity of Evidence

The originality of the evidence is preserved as it is stored with all the participants in the network. The evidence itself is not passed as data in the chain; rather, a hash value is passed.

4. Role Of Blockchain For Digital Forensics

4.1 Super Important Recordkeeping:

So, blockchain is all about being unchangeable. Once something goes on the blockchain, it's like set in stone - very hard to mess with. This is key for keeping all that digital evidence safe and sound

4.2 Keeping Things in Line:

Blockchain helps create a solid chain of custody for digital evidence. Every step of an investigation can be tracked from start to finish, showing exactly what happened along the way. This makes sure the evidence hasn't been messed with.

4.3 Keeping Data Safe:

With blockchain, digital data stays secure with special codes and checks to make sure no one messes around with it. This makes sure everything stays true and honest during a forensic investigation.

4.4 Time is Everything:

Blockchain makes sure every piece of evidence gets a specific time stamp. This is really important in investigations where knowing when things happened is a big deal. The decentralized part of blockchain means these time stamps are super reliable and can't be changed.

4.5 No Weak Links Here:

Because blockchain doesn't have one main spot where things are stored, there's no one place for bad stuff to happen. Data is spread out across lots of places making it tough for anyone to mess with it or lose it.

4.6 Being Sure About Things:

Blockchain helps show if evidence is legit or not by using smart contracts to control who gets to see what info. Only certain people can get into sensitive stuff - pretty smart, huh?

4.7 Open or Private:

Some blockchains let everyone see what's going on (public), while others keep things between a select few (private). Both ways have their uses depending on who needs to know what.

4.8 Smart Contracts :

These are like super helpful agreements written in computer code that can handle tasks on their own - like making sure rules are followed when handling evidence during an investigation.

4.9 Working Together Better:

Blockchain helps different groups work together securely during investigations by sharing info safely and honestly, building trust between everyone involved.

4.10 Keeping an Eye on Cryptocurrency:

For cases dealing with digital money, blockchain really shines bright because it shows exactly where funds go and who's involved in any shady business activities.

5. Objectives

1. Securing Evidence Integrity:

Maintain the trustworthiness of digital evidence by using blockchain's tamper-proof nature, ensuring that evidence remains unchanged and reliable.

2. Establishing Chain of Custody:

Create a secure, transparent, and traceable record of how evidence has been handled or accessed, ensuring its integrity throughout the investigation process.

3. Enhancing Data Authenticity:

Ensure that digital data and evidence are genuine and not altered, providing a verified record of their origin and history.

4. Improving Investigation Efficiency: Utilize blockchain's transparency and efficiency to streamline and accelerate digital forensic procedures, making investigations faster and more reliable.

5.FacilitatingCross-Border Collaboration: Enable easier sharing and verification of digital evidence across different jurisdictions and international boundaries, fostering better cooperation among law enforcement agencies globally.

6.Enabling Standardization:

Develop standardized procedures and protocols for handling digital evidence using blockchain, ensuring consistency and reliability across investigations.

Reference number	Security Evidence Integrity	Establishing CoC	Enhancing Data Authenticity	Improving Investigation Efficiency	Facilitating Cross-Border Collabration	Enabling Standardization
[1]	✓	✓	✓	--	--	--
[2]	--	✓	--	✓	✓	--
[3]	✓	--	✓	✓	--	✓
[4]	✓	✓	✓	--	--	✓
[5]	✓	✓	✓	--	--	✓
[6]	✓	✓	✓	✓	✓	--
[7]	✓	--	✓	✓	✓	--
[8]	✓	✓	--	--	✓	--
[9]	--	--	✓	✓	--	✓
[10]	✓	✓	✓	✓	--	✓

6. Challenges

6.1 Tokenization of artifacts from digital evidence

Tokenization of artifacts from digital evidence is a big task. It involves breaking down evidence into different parts for analysis. Each piece might need to be looked by various people, focusing on different aspects like log files, file systems, or specific binaries that need reverse engineering.

6.2 Efficient management of data volume in the chain of custody.

Managing data volume in the chain of custody is another concern. With thousands of multimedia and log files per case, storing raw documents off-chain using technologies like IPFS or Storj helps. Only hashes should be used in the blockchain for ease of auditability.

6.3 Parse forensic sound procedures in blockchain systems:

It's essential to follow forensic procedures properly when using blockchain. Having standardized flows and smart contracts to ensure verifiability and tamper-proof guarantees is crucial for final validation in court.

6.4 Enable an understandable forensic outcome/reports:

Creating understandable forensic reports is vital. Blockchain offers benefits like efficient data provision, but efforts are needed to make the outcomes user-friendly and court-ready.

6.5 Interoperability and cross-border jurisdictions:

Interoperability and cross-border issues are also significant. Standardized flows and data agreements across borders help combat cybercrime effectively.

6.6 Timeline of events and chronology:

Maintaining a timeline of events is key in digital forensics to identify patterns and prevent future incidents. Blockchain's immutability can help prove data existence at specific times, ensuring evidence integrity.

7.Concluding Remarks

Blockchain technology, with its attributes of transparency and immutability, offers significant potential in digital forensics. It enhances the credibility of digital evidence by providing secure and tamper-proof storage. However, challenges like scalability and technical complexities persist, impacting its seamless integration into forensic practices. As blockchain continues to evolve, addressing these challenges will be crucial for maximizing its benefits in the realm of digital investigations.

In current digital forensics investigations, the preservation of data integrity is carried out independently by central authorities such as prosecutors. Blockchain helps reduce friction through increased trust, offering real promise for the forensic community. Future work aims at developing a complete Ethereum-based intelligent digital forensic chain of custody using smart contracts.

References

[1] Dr.S. Harihara gopalan, S. Akila suba, C. Ashmithashree, a. Gayathri, V. Jebin Andrews, Digital forensics using blockchain

[2] Al-Khateeb, H., Epiphaniou, G., & Daly, H. (2019). Blockchain for modern digital forensics: The chain-of-custody as a distributed ledger. In Advanced Sciences and Technologies for Security Applications

[3] Casino, F., Dasaklis, T. K., & Patsakis, C. (2018). A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and Informatics

[4] Shancang li, senior member, Blockchain based digital forensics investigation framework in the internet of things and social systems

[5] S. Bonomi, M. Casini and C. Ciccotelli, "B-CoC: A Blockchain-based Chain of Custody for Evidences Management in Digital Forensics

[6] Haider Al-Khateeb, Gregory Epiphaniou and Herbert Daly, "Blockchain for Modern Digital Forensics: The Chain-of-Custody as a Distributed Ledger" in Advanced Sciences and Technologies for Security Applications, Wolverhampton, UK:University of Wolverhampton

[7] Mohd zaki mas'ud, aslinda hassan, wahidah, A review of digital forensics framework for blockchain in cryptocurrency technology

[8] Mrunali chopade, sana khan, uzma shaikh and renuka pawar, Digital forensics: maintaining chain of custody using blockchain

[9] Mr.S. Nelson M E.,, Mr. S. Karuppusamy B.Tech.,, Mr. K. Ponvasanth B.Tech, Blockchain based digital forensics investigation framework

[10] Lone, A. H., & Mir, R. N. (2019). Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger composer