IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 7, July 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307171|

Blockchain Applications in Digital Forensics

Bindu K R[1], Ranjini J M [2], Rohini Y N[3]

Department of Master of Computer Application, Dayananda Sagar College of Engineering, Bengaluru, India

ABSTRACT: Digital forensics and blockchain technology integration opens up new opportunities for improving the dependability, integrity, and transparency of digital evidence. This study examines how blockchain technology might be used in digital forensics and examines how it might change the processes of gathering, preserving, and verifying evidence. The paper looks at the advantages, difficulties, and particular use cases of integrating blockchain technology into forensic procedures.

KEYWORDS: Blockchain, Digital Forensics, Cybersecurity, Timestamping, Data Provenance, Chain of Custody, and Evidence Integrity.

I. INTRODUCTION

Since digital forensics offers the tools to locate, store, examine, and present digital evidence in court, it is an essential component of contemporary investigations. Strong procedures are required to make sure that digital evidence is authentic and unaltered throughout the investigation process due to the increasing reliance on digital data across a number of industries, including law enforcement, healthcare, and finance. Even if they work well, traditional digital forensic techniques sometimes have issues with the transparency and integrity of evidence processing. These difficulties include the possibility of tampering, unapproved access, and challenges in confirming the chain of possession [1].

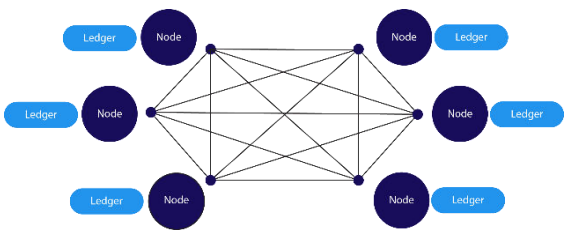
Blockchain technology presents a promising way to address these issues with its decentralized and unchangeable ledger. The immutability, transparency, and decentralization inherent in blockchain technology have the potential to greatly improve the accuracy and dependability of digital forensic procedures [2]. This study looks at how blockchain technology might be used in digital forensics, specifically in terms of how it could change the gathering, preserving, and verifying of evidence.

The significance of authenticity and integrity in digital forensics

In forensic investigations, digital evidence's validity and integrity are crucial. Any modification or tampering with the evidence can compromise the inquiry as a whole, resulting in incorrect convictions or the exoneration of guilty individuals. Conventional techniques for upholding the chain of custody include secure storage and manual recording, both of which are vulnerable to hostile interference and human error. It is extremely difficult to make sure that every piece of evidence is precisely tracked and isn't manipulated from the time it is collected until it is presented in court.

These issues are addressed by blockchain technology, which offers an unchangeable transaction record. Every piece of digital evidence can be registered on a blockchain, which allows for the transparent and impenetrable recording of all actions pertaining to the evidence, including its transmission, collecting, and analysis. This guarantees that any attempt to falsify the evidence will be readily apparent, protecting the digital evidence's validity and integrity throughout the course of the investigation [3].

II. BLOCKCHAIN OVERVIEW WHAT IS BLOCKCHAIN?



International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

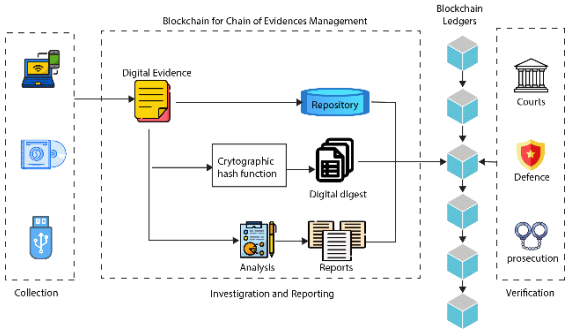
Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307171|

Key Features

- **Decentralization**: Gets rid of the requirement for a centralized government.
- **Immutability**: Data in a block cannot be altered once it has been recorded.
- **Transparency**: Every member of the network can see transactions.
- **Security**: Data confidentiality and integrity are guaranteed by cryptographic procedures.

III. APPLICATIONS IN DIGITAL FORENSICS



Evidence Coherence and Custodial Chain

A key component of forensic investigation is the chain of custody's integrity. It guarantees that the evidence initially gathered is the same as the evidence presented in court. The chain of custody should not have any holes or irregularities as this could compromise the validity of the evidence. A strong solution to this issue is provided by blockchain technology, which delivers a tamper-proof record of all acts made with the evidence [4].

Use Case: Management of the Chain of Custody

- **Implementation:**
  - Every piece of evidence has a unique tag attached to it (like a cryptographic hash). Next, the blockchain records this identifier.
  - Every time the evidence is moved, examined, or accessed, a new transaction is made on the blockchain and documented.
  - A new hash and timestamp are generated for each alteration to the evidence that is made later, and they are also stored on the blockchain.
- **Benefits:**
  - Verifiability: Offers an unchangeable and verifiable history of the creation and modification dates of the evidence.
  - The ability of timestamps to be challenged or changed is known as non-repudiation, and it is essential for creating chronologies in investigations.
  - Tracking the provenance of evidence helps to confirm its integrity and authenticity by making it easier to trace its beginnings and history.

Safe Digital Archiving of Evidence

One of the biggest challenges in digital forensics is securely storing digital data. Conventional storage techniques are susceptible to manipulation and unwanted access. Evidence hashes can be securely stored using blockchain technology, guaranteeing the evidence's integrity throughout time [5].

Use Case: Verification and Storage of Evidence

- **Implementation:**
  - The blockchain stores hashes of digital evidence, guaranteeing that any changes made to the evidence will produce a new hash.
  - Every transaction has specifics like the time and date, who is managing the evidence, and what was done.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307171|

- **Benefits:**
  - Integrity: Once a transaction is recorded, it cannot be changed or removed thanks to blockchain's immutability. This facilitates the detection of any tampering or unwanted access.
  - Transparency: An auditable and transparent trail of evidence handling is provided by the visibility of all transactions to authorized parties.
  - confidence: Establishes a trustworthy and verifiable chain of custody, which increases confidence among stakeholders (such as law enforcement, legal professionals, and courts).

Timing and the Source of Data

In forensic investigations, pinpointing the precise moment of creation, modification, or access to digital evidence is essential. The intrinsic timestamping feature of blockchain makes sure that these important information are reliably recorded and unchangeable.

Use Case: Digital Evidence Timestamping

- **Implementation:**
  - A distinct digital fingerprint is produced by hashing digital evidence. Next, a timestamp and this hash are added to the blockchain record.
  - In a safe area, the actual digital evidence is kept off-chain. By comparing this evidence's hash with the one on the blockchain, its integrity may be confirmed at any time.

- **Benefits:**
  - Integrity Assurance: Any modification to the evidence will result in a different hash, which will differ from the hash on the blockchain and point to manipulation.
  - Security: Since the real evidence is kept safe in a secure environment, storing merely hashes on the blockchain lowers storage needs and improves security.
  - Accessibility: Without having to view the original data, authorized parties can always confirm the accuracy of the evidence.

Intelligent Contracts for Streamlined Procedures

Self-executing contracts, or smart contracts, have the conditions of the contract explicitly encoded into the code. Smart contracts can be used in digital forensics to automate and enforce forensic methods, guaranteeing consistency and lowering the possibility of human error [6].

Use Case: Automated Forensic Protocols

- **Implementation:**
  - Smart contracts are designed to carry out particular forensic operations on their own. For instance, the smart contract can automatically record the transaction, update the chain of custody, and alert pertinent parties when evidence is moved from one party to another.
  - In order to guarantee that all procedures are done correctly, these contracts can also require adherence to forensic standards and guidelines.
- **Benefits:**
  - Ensures that forensic processes are followed consistently, which lowers unpredictability and human error.
  - Efficiency: Automates monotonous jobs so that forensic specialists can concentrate on more intricate parts of the inquiry.
  - Openness and Accountability: Increases openness and accountability by giving a transparent, auditable record of every action taken by the smart contract.

IV. CHALLENGES AND LIMITATIONS SCALABILITY

Blockchain networks may experience scalability problems, especially when there are a lot of transactions. Each node's storage and processing needs rise as the blockchain gets bigger, which could result in longer transaction delays and more expensive fees [7].

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307171|

Privacy Concerns
Since transactions on public blockchains are visible to all network users, privacy concerns may arise. Private or permissioned blockchains, where access is limited and transactions are viewable to only authorized parties, can be used to solve this [8].

Legal and Regulatory Issues
Depending on the jurisdiction, blockchain recordings may or may not be accepted in court. Adoption of technology is accompanied by regulatory hurdles, such as maintaining compliance with standards for electronic evidence and data protection regulations [9].

Integration with Existing Systems
It can be difficult and need major changes to integrate blockchain with the digital forensic systems and technologies that are now in use. Additional difficulties may arise from compatibility problems and the requirement for new protocols and interfaces [10].

V. FUTURE DIRECTIONS CREATING UNIFORM STRUCTURES

Creating uniform frameworks for the application of blockchain technology in digital forensics need to be the main goal of future study. Interoperability, data standards, and best practices for implementation should all be covered by these frameworks.

Hybrid Methodologies
Investigating hybrid strategies that integrate blockchain with other cutting- edge technologies, like the Internet of Things (IoT) and artificial intelligence (AI), could improve digital forensics even more. AI algorithms have the potential to examine enormous datasets stored on blockchains, for instance, while IoT devices offer real-time data collecting and verification.

Better Solutions for Scalability
The shortcomings of present blockchain systems may be addressed and they may become more appropriate for forensic applications through research into enhanced scalability options for blockchain networks, such as sharding, sidechains, and off-chain transactions.

Policy and Legal Aspects to Take into Account
The legal and regulatory obstacles associated with the use of blockchain in digital forensics must be addressed by constant communication between engineers, legal specialists, and legislators. Clear rules and regulations must be established if blockchain technology is to be widely used in this industry.

VI. CONCLUSION

Blockchain technology offers safe, transparent, and unchangeable methods for organizing digital data, which has a huge potential for advancements in digital forensics. Even though there are obstacles to its implementation, continued research and developments should help to resolve these problems and open the door for stronger forensic procedures. In order to improve digital forensics, future study should concentrate on creating standardized frameworks and investigating hybrid strategies that include blockchain with other cutting-edge technology.

REFERENCES

1. Dass, R., and T. Reddy (2017). New Trends and Analysis in Digital Forensics. International Journal of Information Security and Computer Science, 15(2).
2. In 2008, Nakamoto, S. A peer-to-peer electronic cash system is called bitcoin.
3. Nathan, O., Pentland, A., and Zyskind, G. (2015). Decentralizing privacy: securing personal information with blockchain technology. IEEE Security and Privacy Workshops, 2015. Pages 180–184. IEEE.
4. N. Kshetri (2017). The functions of blockchain in enhancing privacy protection and cybersecurity. Policy for Telecommunications, 41(10), 1027–1038.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307171|

5. Bashir, M., and Huang, Y. (2020). Blockchain Technology for Cloud Environments to Provide Secure Data Sharing. Systems of Information, 94, 101610.
6. Ohtsuki, T., Toyoda, K., Mathiopoulos, P. T., & Shen, X. (2017). A new product ownership management system (POMS) for post-supply chain anti-counterfeiting that is built on blockchain technology. 5 (17465–17477) IEEE Access.
7. Wu, Y., Chen, X., and Yang, C. (2018). A comprehensive examination of managing IoT data with blockchain technology. 2018's IEEE Cyber, Physical and Social Computing (CPSCom), IEEE Green Computing and Communications (GreenCom), IEEE International Conference on the Internet of Things (iThings), and IEEE Smart Data (SmartData) (pp. 221-226). IEEE.
8. J. H. Park and Park, J. H. (2017). Blockchain security in cloud computing: Use cases, difficulties, and solutions. 9(8) Symmetry, 164.
9. In 2019, Deuber, D., McGrew, R., and Magazzeni, D. The anatomy of a cryptocurrency attack and its security implications are discussed in Attacking the Blockchain. Pages. 58–72 in the 2019 IEEE European Symposium on Security and Privacy (EuroS&P). IEEE.
10. O'Sullivan, T., Lillis, D., Becker, B., & Scanlon, M. (2016). Future directions for digital forensic investigative study as well as existing difficulties. Preprint arXiv:1604.03850; arXiv.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details