RESEARCH ARTICLE

RSP Science Hub

International Research Journal on Advanced Science Hub
2582-4376
www.rspsciencehub.com
Vol. 07, Issue 06 June

Check for updates

http://dx.doi.org/10.47392/IRJASH.2025.061

A Review of Different Blockchain-Based Mechanisms Incorporated for Enhancing Data Security in Digital Forensic Images

Mr. Koushik R[1], *Dr. Vikas S*[2]

[1]*Research scholar, Dept. of CSE, VTU CPGS Mysuru, Karnataka, India.*

[2]*Assistant professor, Dept. of CSE, VTU CPGS Mysuru, Karnataka, India.*

Email ID: *koushikrnaik7@gmail.com*[1], *vikas.smg@gmail.com*[2]

Article history

Received: 08 May 2025
Accepted: 19 May 2025
Published: 27 June 2025

Keywords:

Blockchain, Digital Forensics, Data Security, Forensic Images, Immutability, Cryptography.

Abstract

Digital forensics plays a crucial role in criminal investigations, cybersecurity, and legal proceedings. Ensuring the integrity and authenticity of digital forensic images is paramount to maintaining evidentiary value. Traditional methods of securing forensic data face challenges such as tampering, unauthorized access, and lack of transparency. Blockchain technology, with its decentralized, immutable, and cryptographic properties, offers a promising solution to enhance data security in digital forensic images. This paper reviews various blockchain-based mechanisms that have been incorporated to improve the security, integrity, and traceability of forensic images. We discuss different blockchain architectures, consensus mechanisms, and cryptographic techniques employed in forensic applications. Additionally, we highlight challenges and future research directions in this domain.

1. Introduction

Digital forensic image is an exact replica of a storage media and serves as a recalls of evidence for criminal investigations, cyber security incidents and for court cases. These images must be kept intact in the interest of the integrity of such images and because any improper modifications discourage use of evidence in the courts. However, cryptographic hashing (e.g., MD5, SHA-256) and centralized storage systems are a very traditional method used on preserving forensic data. These techniques offer a minimum level of security but suffer from a single points of failure, insider threats, and tampering, which causes one to question the reliability of digital evidence in the Court. Further, centralized systems are not transparent, which is problematic nationally because it makes it difficult to verify the chain of custody and also detect unauthorized alterations after acquisition. Introduced as a means to secure data in criminal examinations and raise the losses of those involved, Blockchain technology at the beginning was developed for decentralized cryptocurrencies like Bitcoin. Using blockchain's inherent characteristics; decentralized, immutable, and with cryptographic verification, blockchain could help with restrictions of traditional forensic storage protocols. A forensic image hash is recorded in a tamper proof blockchain based ledger so that the data integrity can be verified in real time. Furthermore, through smart contracts, access control can be automated to some extent, and the audit trail is decentralized with IPFS as an example of InterPlanetary File System (IPFS) that can store and manage forensic datasets securely while avoiding vulnerable central servers. In this paper, we describe different blockchain based mechanisms to strengthen the security of digital forensic images. Cryptography is used for verifying the hash, smart contract is used for guarding the chain of custody, and making use of decentralized storage solutions is used to avoid data manipulation. Consequently, on the one hand we study different blockchain architectures, public, private or consortium, and all the associated consensus mechanisms (e.g. Proof of Work, Proof of Stake, Pratical Byzantine Fault Tolerance), in order to assess if they are scalable for forensic applications. Blockchain brings in many advantages but we are constrained by the problems in scalability, computational overhead and legal admissibility when blockchain is used in digital forensics. To employ the blockchain in forensic investigations on a vast scale, these issues should be resolved first. This paper attempts to provide an all round perspective on blockchain technology as well as assess how it can be used to convert digital forensic security into blanket security for the blockchain based digital infrastructure, based on how existing frameworks and existing research rate. Finally, future directions of this kind — hybrid blockchain models, lightweight consensus algorithms and AI assisted forensic validation — are also briefly discussed to guide future developments in that space. This is a positive for the blockchain set up to be a more transparent, hardened, and auditable digital forensic evidence storage system.

2. Blockchain Technology in Digital Forensics

2.1. Fundamentals of Blockchain

A distributed ledger technology (DLT), blockchain is a technology that enables secure, transparent and tamper proof record of transaction across a decentralized network. Unlike virtual centralized databases, blockchain works as a peer to peer (P2P) network wherein every single node stores a copy of the ledger. This architecture also ensures that if we were to be delivered with food poisoning for example, no entity can take control of the whole system, which would massively decrease the risk of data manipulation, or single point failure. Given that the core principles of the blockchain—decentralization, immutability, and cryptographic security—are ideally suited for strengthening the integrity and authenticity of a digital forensic image, its adoption within the realm is quite expected. Another core property of blockchain that destroys its dependency on a central authority is it is decentralized. Centralized servers or databases can make such storage vulnerable to cyberattacks, insider threat, or administrative errors, which are frequent in digital forensics. Because blockchain is essentially decentralized, forensic data is spread accross multiple nodes which makes it impossible for someone to modify that data while also making it much more impossible for a cyber-attack to ‘destroy’ data. For instance, when a forensic investigator acquires an image of a relevant disk to be used as evidence, the storing of the metadata on a blockchain (e.g., hash value, dates) will ensure that only when consensus is reached with the entire network can that single entity change the record. Immutability is a characteristic that enables us to write data on the blockchain and to not be able to modify or delete it. The cryptographic hashing, followed by data chaining of blocks, where each block includes the hash of the previous block ensures that there is no possible way to locate blocks without the set of blocks forming a block chain. The requirement of an unalterable chain of custody for forensic images is vital in digital forensics as it ensures the evidentiary value of the forensic images. Investigators store forensic hashes of the evidence (such as SHA-256, MD5) on the blockchain thus ensuring that the evidence has not been tampered since it was acquired. All attempts to change the forensic image would result in a different hash, signaling an immediate difference and keeping the integrity of the trail. Data is authenticated and protected in blockchain with the help of advanced encryption techniques. Transaction or data entry are secured via cryptographic hashing algorithms (e.g., SHA-256), digital signatures, which validate identity of parties involved. In digital forensics, cryptographic mechanisms guarantee that the forensic records can only be accessed by those who have the authorization to do so (e.g., law enforcement persons, forensic analysts). For instance, forensic image can be digitally signed by a forensic investigator, store its hash on the blockchain and be non-repudiate and traceable. Furthermore, forensic workflows like verifying evidence integrity before granting access to authorized users can be made smart contract (self-executing agreements with predefined rules), as well. Incorporating blockchain into the digital forensics will allow the investigators to build up a trustless and auditable environment of securely recorded and verifiable forensic evidence that is admissable in legal courts. The combination of decentralization, immutability, and cryptographic protection to allegations of data tampering, unauthorized access, and lack of transparency, are tackled by it. While blockchain carries many advantages, its introduction to forensics should also take into account some challenges including scalability, computational overhead and compliance with the regulatory obligation, which will be discussed below.

2.2. Blockchain for Forensic Image Integrity

Blockchain technology has been increasingly integrated into digital forensics to enhance the security and integrity of forensic images. Several key approaches have been proposed, each leveraging different aspects of blockchain's decentralized and immutable nature.

2.3. Hash-Based Verification

Hash based verification is one of the most commonly used mechanism of securing forensic images using blockchain. In this approach first forensic images are crypto graphically hashed (such as MD5, SHA-256) and subsequently these hashes are stored time bounded on the blockchain. As blockchain is immutable, a hash that has been recorded cannot be changed without detection. If any accidental or malicious modification is made to the forensic image, the hash value will change every time, indicating thereby tampering. This ensures that forensic investigators can look at the image whose hash is provided and compare it with the hash saved on the blockchain as to verify it is authentic. This is then put into action in a practiceable chain of custody system that is implemented as a blockchain and uses the chain for a series of blocks to include the forensic image hash, timestamps, and fingerprint. This leads to a transparent and auditable trail as anything tampered with should be caught early on during a investigation.

2.4. Smart Contracts for Automated Verification

However, a more automated approach to verifying forensic data integrity can be reached by using smart contracts, or self-executing agreements with predefined rules both of which are encoded on the blockchain. Forensic images can be able to be programmed to be checked upon the hashes being checked against the hashes stored in the blockchain based on letting in or over modifications. Let's take for instance if a smart contract was designed to make access to a forensic image possible if the hash of said image matched the one engraved on the blockchain so that only unaltered evidence could be used in investigation. Moreover, smart contracts can enact policies regarding access control and the only personnel who are allowed to access (retrieve, modify) forensic data are authorized personnel (e.g., forensic analysts, law enforcement). This reduces human error and reduces the possibilities of tampering with digital evidence in legal proceedings by unauthorized people. (Figure 1)

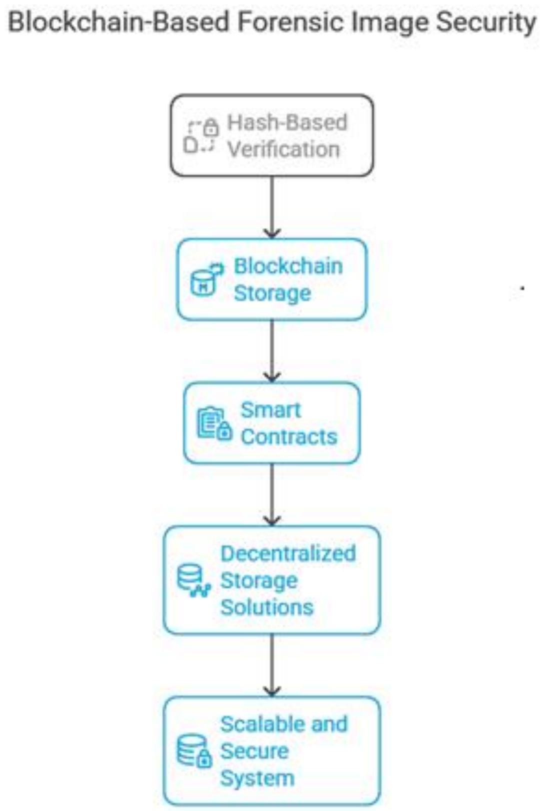
Blockchain-Based Forensic Image Security
Hash-Based Verification
Blockchain Storage
Smart Contracts
Decentralized Storage Solutions
Scalable and Secure System

Figure 1 Blockchain-Based Forensic Image Security

2.5. Decentralized Storage Solutions

As a matter of fact, storing large forensic images directly on a blockchain cannot be done often due to scalability limitations. In order to remedy this, InterPlanetary File System (IPFS) provides its own decentralized storage solutions in combination with blockchain. Here, forensic images are stored off chain in IPFS that supports distributed and redundant storage while the metadata of them (i.e., cryptographic hashes, timestamps, ownership details) are stored on the blockchain. Because forensic images are stored with content-addressable storage (wherein files are retrieved by hash) which is used in IPFS, if the image is tampered with, the hash used by IPFS to retrieve it changes, making tampering discoverable. The use of blockchain for verification and IPFS for storing large amounts of data makes this approach both highly efficient in storage and highly secure. For example, a real world application could involve law enforcement agencies uploading forensic rewrite of forensic images to IPFS and record their hashes on a permissiond blockchain to make sure that the evidence is secure, verifiable and easily accessible to the prosecution only. These blockchain mechanisms as a whole promote the security, transparency, and reliability of digital forensic images by addressing concerns that data has been tampered with or not, and no one has permission to enter or exit the encrypted image at any moment in time, and dealing with concerns of data chain-of-custody. An option for future advancement may come in the optimization of these approaches towards the attainment of scalability, interoperability, and certainly the compliance with given legal issues that may arise when the use will also be used in digital forensics. [1]

3. Blockchain Architectures for Digital Forensics

Various forms of blockchain technology have been adapted to serve the specific scenes of digital forensics. Different blockchain models bring different advantages and tradeoffs in respect to transparency, security, speed and control. Subsequently, two Forks of public and private blockchains have been listed for forensic applications and their consequences for forensic data integrity and accessible. [2]

3.1. Public vs. Private Blockchains

Public blockchains like Ethereum and Bitcoin utilize any node in order to partake in the network in a fully decentralized setting. As these are very transparent because all transactions are made open for verification by any one of the parties involved, they are immune from being tampered or defrauded. While PoW kind of mechanisms can be associated with, they burden unnecessary computational and latency overhead which might be a not so good thing in the context of time bound forensic investigations. Moreover, the privacy of the public block chains regime may be compromised when dealing with such forensic data since all the transaction details are disclosed to everyone. Alternatively, all the private blockchains such as the ones in Hyperledger Fabric and R3 Corda, are permissioned networks with the access governed by authorized entities i.e., law enforcement agencies and the forensic investigators. And they are more useful for forensic applications where confidentiality is important because they facilitate more control of access to data and over data modification. Private blocks are slower than regular chains so private chains typically use faster consensus therefore like PBFT, etc. to reduce the time that is taken to reach the consensus. The information has been designated as structured data element in order to make them more efficient for real time forensic evidence logging and chain of custody tracking. This, however, is still a centralized thing, but it still leaves people who govern the blockchain with possible trust dependencies, defeating the advantage of decentralization in blockchain.

3.2. Consensus Mechanisms in Forensic Blockchain Systems

The choice of consensus mechanism plays a pivotal role in determining the efficiency, security, and suitability of a blockchain for forensic applications. Three prominent consensus models have been explored in this context:

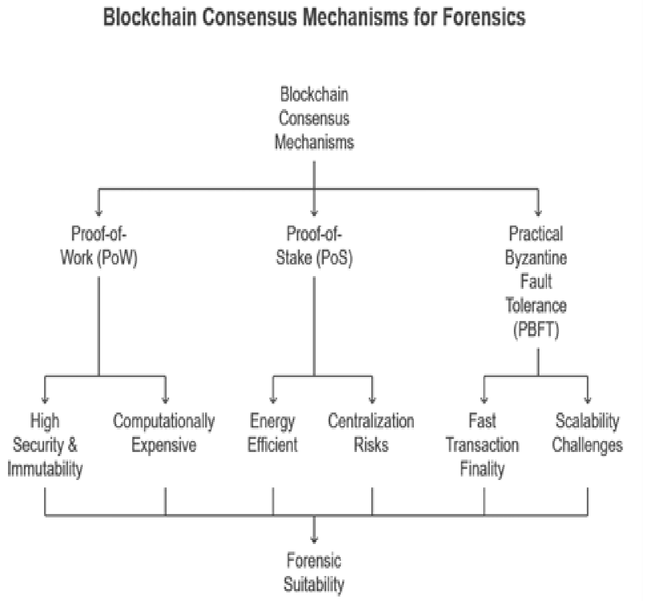
Blockchain Consensus Mechanisms for Forensics
Blockchain Consensus Mechanisms
Proof-of-Work (PoW)
Proof-of-Stake (PoS)
Practical Byzantine Fault Tolerance (PBFT)
High Security & Immutability
Computationally Expensive
Energy Efficient
Centralization Risks
Fast Transaction Finality
Scalability Challenges
Forensic Suitability

Figure 2 **Blockchain Consensus Mechanisms for Forensics**

Proof-of-Work (PoW): In Bitcoin and also in early Ethereum, PoW was first used where miners are required to solve a complex cryptographic problem in order to validate transactions and append a block to the chain. PoW, while computationally expensive and energy intensive, provides a security and immutability which are necessary for securing the forensic evidence integrity. While PoW blockchains are not practical for large scale forensic evidence management (e.g. slow transaction throughput, Bitcoin's ~7 TPS), the deleted data problem is due to PoS blockchains and that can remedied. [4]

Proof-of-Stake (PoS): PoS replaces computational power as the main factor in being a validator with stake, i.e., cryptocurrency holdings. Ethereum 2.0 shows that, apart from offering security, a PoS approach could lead to a reduction in energy consumption for Ethereum. Yet, with that PoS brings concerns of centralization — wealthier participants can cast a larger vote in influencing consensus. This means that in case of for applications, if one entity has a majority of the staking power, trust issues could arise.

Practical Byzantine Fault Tolerance (PBFT): In fact, as only a limited number of stubborn nodes exists in a permissioned forensic network, PBFT is commonly used in private and consortium blockchains. Despite malicious nodes, PBFT can guarantee fast transaction finality (within seconds) and resiliency against them if it is honest at least two-thirds the network. Therefore it is ideal for law enforcement and forensics agencies that need to log evidence rapidly and audibly while incurring minimal computational burden of PoW. Nevertheless, the assumption of PBFT that it is run on a fixed set of validators may impose a limitation on the scalability of PBFT in large, dynamic forensic environments. [5]

3.3. Comparative Analysis and Forensic Suitability

With forensic applications, private blockchains with PBFT or PoA (Proof of Authority) consensus are very much preferences as they provide good speed, security, and controlled access. On the other hand, public blockchains are so tamper resistant that they would make excellent Francisco forensic evidence, but are not so scalable or private enough for real Francisco forensic evidence management. Future work could explore hybrid models that combine the transparency in public ledgers and the efficiency of private networks in maintaining the balance of security and performance of a forensic data.

This section highlights the importance of selecting an appropriate blockchain architecture and consensus mechanism based on the specific requirements of digital forensics, ensuring both data integrity and operational efficiency. [3]

4. Challenges and Limitations

While the advantages of combining the uses of blockchain technology in enhancing security and integrity of digital forensic images are significant; however, there are still several challenges that prevent the use of blockchain technology in the field of digital forensic investigation. The most critical aspect of all these is scalability. Large storage devices can make forensic images several terabytes in size. Since blockchain storage capacity is limited and the costs associated with it cannot scale together with the size of the storage required, storing such massive datasets on a blockchain is impractical. For example, off-chain storage (e.g., IPFS) combined with on-chain hashes do solve this problem, though it unfortunately comes with additional layer of complexity of making data available and instantiable. Legal admissibility is another important obstacle. Digital evidence is used by courts and legal systems, so they have had well established procedures to verify the authenticity and reliability of such evidence. While blockchain technology is new to the forensic applications, legal structures are not clear about whether it can be used as evidence because it is new. Some of the questions around the validity of blockchain logs that provide you with a way to prove what cannot be proved otherwise, how you can guarantee that consensus is reaching some worldwide definite decision, are you going to have lines that are always true, so there's no vulnerability in your smart contract. To be accepted by the bench, blockchain based forensic solutions necessitate that standardized protocols and certifications are developed, which would align with the legal requirements. The second limitation is that computational overhead scales badly with nodes, especially in networks like blockchain that use energy consuming methods of proof of work (PoW) for consensus. Fast transaction speed and high energy consuming issue is characteristic for PoW based blockchains (e.g., Bitcoin), which makes forensic investigations unnecessarily time consuming. Other alternative models of consensus such as Proof of Stake (PoS) or Practical Byzantine Fault Tolerance (PBFT) trade efficiency for some degree of decentralization or security. Even to this day, the opportunity for optimizing blockchain architectures for forensic use cases is a live research challenge. Measures include integrating data requirements specification among public safety agencies, encouraging the establishment of a single data standard, aiding with compatibility between various types of database and ensuring interoperability between various public safety agencies. This is because that digital forensics includes many tools and platforms (for example EnCase, FTK, Autopsy) and each of them has its own formats and workflows which proprietary. Blockchain forensic solutions have to be compatible with existing forensic tools for evidence collection, analysis and report. Added to this, different blockchain platforms (i.e. Ethereum vs. Hyperledger), present further list of complications when it comes to interoperability due to lack of standardization. Solution to these challenges will be drawn from collaborations between researchers, forensic practitioners, legal experts and developers of Blockchain. In order to move forward with understanding blockchain as a trusted digital forensic security mechanism, future advancement in such phenomena as hybrid blockchain architecture, lightweight consensus model and regulatory framework will overcome the aforementioned barriers, and enable blockchain as an established solution in the field. [6]

5. Future Research Direction

Hybrid Blockchain Solutions: Combining On-Chain Hashes with Off-Chain Storage Hybrid solutions that apply on-chain and off-chain storage mechanisms are considered as one of the most promising in blockchain based digital forensics. Because blockchain networks are designed for low scale data storage, it is impractical to store whole forensic images directly on a blockchain. A hybrid approach rather lays down in the blockchain only cryptographic hashes of forensic images (like SHA-256, or MD5), and leaves the original image in distributed off chain storage systems, such as the Inter Planetary File System (IPFS) or distributed cloud storage. With this, the data integrity is maintained, hence any modification of the Forex image will lead to change of the hash making tampering immediately detectable. Furthermore, forensic evidence can be made accessible and later modified via verification or retrieval processes only to authorized entities via the use of smart contracts for automation. The hybrid model has good security, efficiency, and cost effectiveness and is a solution for law enforcement and forensic investigators. [7]

Lightweight Consensus Algorithms: Reducing Computational Overhead PoW suffers from high computational and energy inefficiencies, which are critical disadvantages for real time forensic applications and make them impractical to serve real time forensic applications. About this, researchers are exploring how consensus can be made ‘lighter’ —exus, to México — by using Proof of Stake (PoS), Delegated Proof of Stake (DPoS), or Practical Byzantine Fault Tolerance (PBFT). Keeping security as always on high level, these alternatives reduce energy consumption and transaction latency. An example of how much computational overhead is required is that PoS-based blockchains require validators to stake cryptocurrency as opposed to solving complex mathematical puzzles, and it makes it much easier to stake since validators do not have to maintain high computational power to compete. Lightweight consensus is critical for forensic applications where data integrity must not be sacrificed for time efficiency, and in such cases, consensus models can improve efficiency. Future research should also focus on parametrization of these algorithms so that they conform to the high security demand of legal and investigative processes. [8]

Standardization Efforts: Establishing Legal and Technical Standards for Blockchain Forensics

In spite of the advantages of blockchain in digital forensics, widespread adoption of blockchains in digital forensics faces the barriers of lack of standardized protocols and legal frameworks. Currently different legal standards exist for admissibility of digital evidence in different jurisdictions and therefore, blockchain forensic solutions must be compliant to these legal standards for all those to be accepted in the court. Standardization efforts should focus on:

- **Technical Standards:** Defining uniform blockchain architectures, cryptographic hashing methods, and data storage protocols to ensure interoperability between forensic tools.
- **Legal Admissibility Guidelines:** Establishing clear legal precedents and certification processes for blockchain-based forensic evidence, ensuring courts recognize its validity.
- **Forensic Certification Programs:**

Developing training and certification programs for forensic experts to ensure proper implementation and verification of blockchain-secured evidence. [9]

Organizations such as NIST (National Institute of Standards and Technology) and ISO (International Organization for Standardization) are beginning to explore blockchain forensics standards, but further collaboration between technologists, legal experts, and law enforcement is essential for creating a globally accepted framework.

Conclusion

Digital forensic images have been found to be susceptible to numerous attacks and have therefore become bot susceptible to hacking and rampant forgery. This paper shows how autonomous forensic evidence management can be provided using decentralized, cryptographic hashing, and smart contracts with blockchain's features: tamper proof and auditable. Blockchain is decentralized and completely removes the points of failure throughout the lifecycle of any forensic image, ensuring that the same remains unaltered. Forensic data cryptographic hashing (SHA-256) guarantees that the modification of any remote sample data will immediately manifest as noncompliance of the forensic protocol, while smart contracts help automate the verification process, which in turn will minimize the error from the conduct of forensic protocol and comply with the forensic protocol. In addition, the immutable ledger of blockchain simplifies the validation of the authenticity of the chain of custody by investigators, legal authorities, etc. Though these advantages could contribute to the widespread application of blockchain in digital forensics, some challenges make the way less easy. However, it remains a critical problem that images contained on the forensic images so large that they can't be stored on chain due to storage constraints and latency on transactions. It is also a matter of legal admissibility that courts may need to validate further blockchain based forensic mechanisms before accepting them as standard evidence. This, in addition to the computational overhead represented by Proof of Work (PoW) consensus algorithms is an efficiency challenge in the forensic environment that is resource constrained. This is where future research picks up from the shortcomings of this approach and investigate hybrid blockchain architectures and handle it by storing metadata on chain and off chain forensic data such as decentralized file systems (e.g. IPFS). Besides Proof-of-Stake (PoS), or Practical Byzantine Fault Tolerance (PBFT) other lightweight consensus mechanisms that reduce energy use and speed up transactions were also a possibility. In addition, the integration of AI into the blockchain based forensic systems can be also used to detect automatic tamper detection and anomaly analysis. As much as the work in this paper is shared by the forensic institutes, the legal bodies and the blockchain developers, then all the parties will have to take standardsization efforts to establish universally accepted frameworks for the digital forensics based on blockchain. However, blockchain can finally be used to overhaul digital forensics with the idea that data should be secure, transparent and should not be hacked. In order to accomplish this, however, it will encounter technical and legal hurdles in bringing it to completion. The future presents us with better hybrid blockchain models, very refined consensus algorithms, and the fruitful interdiciplinary collaboration will bring in more efficient and legally admissible forensic solutions. [10]

References

[1]. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

[2]. Taylor, P. J., Dargahi, T., Dehghantanha, A., & Choo, K. K. R. (2019). A Systematic Literature Review of Blockchain Cyber Security. IEEE Access.

[3]. Kaur, H., & Alam, M. A. (2021). Blockchain-Based Forensic Framework for Secure Digital Evidence Management. Journal of Network and Computer Applications.

[4]. Zikratov, I., Kuzmin, A., Akimenko, V., & Niculichev, D. (2017). Ensuring Data Integrity Using Blockchain Technology. IEEE 20th Conference on Business Informatics.

[5]. Le-Khac, N. A., & Kechadi, M. T. (2020). Blockchain for Digital Forensics: Challenges and Opportunities. Springer.

[6]. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf

[7]. Kaur, H., & Alam, M. A. (2021). Blockchain-Based Forensic Framework for Secure Digital Evidence Management.

Journal of Network and Computer Applications, 185, 103-117. https://doi.org/10.1016/j.jnca.2021.103117

[8]. Le-Khac, N. A., & Kechadi, M. T. (2020). Blockchain for Digital Forensics: Challenges and Opportunities. Springer. https://doi.org/10.1007/978-3-030-38954-3

[9]. Zikratov, I., Kuzmin, A., Akimenko, V., & Niculichev, D. (2017). Ensuring Data Integrity Using Blockchain Technology. IEEE 20th Conference on Business Informatics (CBI), 1, 54-62. https://doi.org/10.1109/CBI.2017.23

[10]. Taylor, P. J., Dargahi, T., Dehghantanha, A., & Choo, K. K. R. (2019). A Systematic Literature Review of Blockchain Cyber Security. IEEE Access, 7, 120858-120878. https://doi.org/10.1109/ACCESS.2019.2928612d