**ABSTRACT**

**INTRODUCTION**

One of the fundamental challenges in the realm of justice is ensuring the integrity and authenticity of evidence used in legal proceedings. Evidence is the bedrock of any fair trial, and the way it is handled can significantly impact the outcome of a case. The management of this evidence is essential to uphold the fairness, transparency, and legitimacy of the judicial process.

In digital forensics, managing evidence is one of the primary challenges. From the moment evidence is collected until it is presented in a legal court, it passes through multiple entities, each of which temporarily assumes ownership. Evidence must not only be collected accurately but also handled in a way that ensures it remains intact and untampered with throughout its lifecycle—from collection and storage to its eventual use in court. This process, known as the Chain of Custody (CoC), validates how evidence has been gathered, tracked, and protected throughout the investigation. Although CoC is not a mandatory step in forensic analysis, it is crucial in ensuring that the evidence remains unaltered, thus making it admissible in legal proceedings. A robust CoC process must adhere to strict standards to handle and preserve evidence, whether digital or physical.

The Chain of Custody refers to the process of documenting the chronological history of evidence, from its acquisition to its presentation in court. This meticulous documentation ensures that evidence has been properly handled and has not been tampered with or altered in any way that could undermine its credibility. The integrity of the CoC is especially important in international criminal trials, where evidence often comes from a wide array of sources, such as national legal systems, non-governmental organizations (NGOs), international organizations, and even private citizens. The diversity of sources and the complexity of the evidence create challenges in maintaining a seamless, secure, and transparent chain that can withstand legal scrutiny.

Historically, the management of the CoC has relied heavily on manual documentation and physical handovers. Each time evidence changes hands—whether during collection, storage, transportation, or presentation—legal authorities document the transfer through signed paper trails and secure handovers. While this method has been effective to some extent, it is not immune to human error, oversight, or, in some cases, deliberate manipulation. These vulnerabilities can compromise the integrity of the evidence and, consequently, the entire legal process. Moreover, as the volume of digital evidence increases, particularly in the form of multimedia content, forensic reports, and electronic records, the limitations of traditional methods become even more apparent.

In recent years, the emergence of blockchain technology has provided an innovative solution to the challenges associated with evidence management, particularly in safeguarding the CoC. Blockchain’s unique characteristics—such as immutability, decentralization, transparency, and traceability—make it an ideal tool for managing the CoC in a way that minimizes the risk of tampering, ensures accountability, and enhances trust among all parties involved. By using a distributed ledger system, blockchain technology allows for the creation of a secure and verifiable record of every transaction or transfer of evidence. Once data is recorded on the blockchain, it cannot be altered without the consensus of all parties involved, ensuring that the integrity of the evidence remains intact throughout its lifecycle.

The immutability of blockchain means that once evidence is logged into the system, its history cannot be changed or deleted, making it highly resistant to tampering or manipulation. This is particularly beneficial for ensuring that the CoC remains unbroken, as each transfer of evidence can be logged with a digital signature, providing an indisputable record of who handled the evidence and when. Furthermore, blockchain's decentralized nature ensures that no single entity or individual has complete control over the evidence, which mitigates the risk of corruption or bias in the process. Every participant in the blockchain network can independently verify the integrity of the evidence, promoting transparency and trust.

The use of smart contracts—self-executing contracts with the terms of the agreement directly written into code—adds another layer of security and efficiency to the process. In the context of evidence management, smart contracts can automate many aspects of the CoC, such as triggering notifications when evidence is transferred or ensuring that only authorized individuals can access certain pieces of evidence. This automation reduces the risk of human error and speeds up the legal process, allowing courts to focus on the substantive aspects of a case rather than administrative details.

In this dissertation, blockchain technology is proposed as the underlying framework for a tamper-proof CoC system that can be applied to the ICC’s judicial process. By integrating blockchain into the evidence management system, this study aims to address the challenges associated with the traditional CoC, particularly in cases involving digital evidence or evidence from multiple parties. The research explores how blockchain can enhance the reliability, traceability, and security of the CoC, thereby ensuring that evidence remains credible and admissible in court.

The study's objectives include validating blockchain as a solution for managing judicial evidence, reviewing existing literature on blockchain's application in legal systems, and designing a blockchain-based architecture that meets the specific requirements of the ICC and other international courts. Ultimately, this research seeks to demonstrate that blockchain can revolutionize the way evidence is managed, not only in international criminal trials but also in other areas of law where the integrity of evidence is paramount.

By exploring blockchain's potential to streamline and secure the CoC, this dissertation contributes to the growing body of knowledge on how technological innovations can enhance judicial processes and ensure that justice is delivered fairly and efficiently in an increasingly complex and interconnected world. The use of blockchain in evidence management is not merely a theoretical concept but a practical solution that can address some of the most pressing challenges facing international courts today, ensuring that the pursuit of justice remains uncompromised by the vulnerabilities of traditional methods.

**lITERATURE REVIEW**

1. Alqahtany, S. S., et al (2024). The empirical evaluation demonstrated that smart contracts are both efficient and practical, with minimal latency and operational overhead. This indicates that the approach can be implemented without significant performance drawbacks. The proposed framework enhances the credibility of forensic evidence in legal settings and offers a flexible model for a wide range of forensic applications, including those in IoT and cloud computing. Ultimately, this research makes a substantial contribution to ensuring the integrity of judicial processes and advancing justice by improving the standards of forensic investigation through the use of blockchain technology.
2. Yao, Q., et al (2024). This paper introduced an image evidence protection framework for forensics, using digital watermarking and blockchain technology. The proposed multi-bit watermarking algorithm, based on self-supervised learning, embeds event-related information into images, making them more resistant to attacks. The watermark, stored in a blockchain smart contract, allows for the verification of both the image and its associated events. While the framework is effective, future research will focus on reducing image distortion, extending to video evidence, and refining the watermark payload size based on image content.
3. Miller, A., et al (2024). This study presents an innovative model to ensure the integrity and preservation of digital evidence, enhancing its admissibility in court. The model, called IntegriStore, leverages blockchain and smart contract technology to manage role-based access control, enabling collaborative investigations without restricting evidence ownership to a single individual. By handling access control via smart contracts, the chain of custody is securely logged, with blockchain states accessible directly from indexed events for smooth integration with external systems. While effective, the model's complexity, particularly the size of the smart contract, may pose management challenges.
4. Dhulavvagol, P. M., et al (2024). The SHARD-FEMF framework was used in this paper to made advanced forensic evidence management and improve efficiency and scalability. It reduced gas consumption, optimizing computational resources and lowering costs. Additionally, it cut time consumption, speeding up the processing of forensic evidence, which is crucial for investigations. SHARD-FEMF also enhances scalability, allowing for better handling of increased evidence volumes without performance loss. With these improvements in efficiency, scalability, and security, the framework offers a valuable solution for managing forensic evidence, supporting law enforcement and the justice system.
5. Santos, N. M. B. R. D. (2024). This paper work focuses on equipping International Criminal Justice institutions with tools like blockchain technology to enhance evidence management and the chain of custody. Using the DSRM approach, the work is divided into four key stages. The first stage identified the value of blockchain in this sector, validated through the Blue Ocean Strategy. The second stage set solution objectives based on a comprehensive literature review. The third and fourth stages involved designing, developing, and demonstrating the MultiTrustBloc framework. In the fifth stage, experts evaluated the solution's usefulness. Finally, the sixth stage confirmed the research's novelty with two approved papers.
6. Batista, D., et al (2023). This research provides a thorough literature review on using blockchain technology to maintain the chain of custody for physical evidence. It identifies a research gap in leveraging blockchain and smart contracts to enhance reliability and integrity in the physical evidence chain of custody. The study concludes that blockchain presents a clear opportunity to mitigate legal risks, ensure compliance, and improve auditing processes. The immutability of blockchain strengthens security and offers a clear, organized view of the evidence lifecycle, benefiting both digital and traditional forensics. Additionally, blockchain could reduce government costs related to public safety and judicial proceedings. The review highlights the need for further research into blockchain's role in evidence management across various sectors, including criminal investigations and industries like Oil & Gas.
7. Shivani, E., et al (2023). The implementation of blockchain technology in forensic evidence management enhances the security, transparency, and immutability of digital evidence. Each piece of evidence is assigned a unique cryptographic hash and recorded on a decentralized, distributed ledger maintained by a network of nodes, preventing any single entity from having control. Smart contracts can automate validation and verification, improving integrity and efficiency. Cryptographic techniques secure sensitive information, while transparency and traceability reduce the risk of evidence tampering. However, scalability challenges and the need for legal and regulatory alignment must be carefully considered to ensure compatibility with forensic procedures.
8. Rana, S. K., et al (2023). This paper presents a decentralized model for protecting digital evidence using smart contracts on the Layer 2 Polygon blockchain. The model leverages blockchain's immutability, transparency, and decentralization to ensure the security and integrity of digital evidence, creating an untrustful, automated system that eliminates intermediaries and reduces the risk of tampering. Experimental evaluation demonstrates the model's efficiency and effectiveness, while the scalable and affordable nature of the Polygon blockchain makes it suitable for real-world applications. However, challenges remain, such as addressing scalability for large volumes of evidence and incorporating advanced cryptographic techniques like zero-knowledge proofs to enhance privacy. Future work should focus on optimizing storage processes, improving usability, and addressing legal and regulatory concerns by collaborating with policymakers to ensure compliance with existing laws.
9. Chougule, H., et al (2022). This work is a prototype software system that uses an access control paradigm for managing data in unsaturated environments. The system's algorithms were implemented with a focus on functionality, acceptability, and manageable complexity. A key feature is the customization of dynamic access policies, which can be modified without requiring additional actions from other members of the system. This eliminates the need for frequent changes to user keys while maintaining the integrity of transaction information, including access grants and changes. Additionally, a blockchain-based system with configurable data encryption permissions is proposed to enhance security.
10. Akhtar, M. S., et al (2022). Digital forensics focuses on investigating electronic evidence, encompassing the detection, acquisition, processing, analysis, and reporting of digital materials. It is essential for law enforcement, as electronic evidence is often involved in unlawful activities. A significant challenge is ensuring data security and integrity, especially with Internet of Things (IoT) devices. To address this, a model is proposed that utilizes blockchain technology and hashing algorithms to maintain security and predict threats. By storing crime evidence on a blockchain and employing Machine Learning models, such as XGBoost, the system achieves early attack detection with accuracy rates of 99.8%, 95%, and 79% for different data types. This approach effectively enhances the integrity and security of digital forensics.
11. Borse, Y., et al (2021). The field of Digital Forensics is evolving, revealing significant differences between managing digital evidence and physical evidence traditionally used in court. Blockchain technology offers crucial features for digital evidence management, including authority, authenticity, integrity, transparency, auditability, and security. It enhances the forensic and scientific chain of custody compared to conventional methods, reducing conflicts through increased trust. Consequently, blockchain presents a viable solution for maintaining the chain of custody of digital evidence, helping to prevent manual errors that could affect its admissibility in court.
12. Tsai, F. C. (2021). The increase in digital evidence due to emerging technologies significantly impacts criminal investigations, necessitating the maintenance of its integrity and authenticity. This study proposes a blockchain-based custody framework to support lawful evidence collection and transfer. It introduces a role for investigators with varying authorization levels to access sensitive cases, combining the roles of creator and owner to ensure rigorous evidence handling. Implemented on the Ethereum blockchain with smart contracts, the framework validates the immutability of evidence data and facilitates effective crime case sharing. Future research may focus on exploring additional roles in investigations and addressing scalability for broader applications.
13. Kim, D., et al (2021). This paper proposes a two-level blockchain system to enhance the integrity and management of digital crime evidence, addressing the risks of damage or manipulation during storage on physical hard disks. The system allows only authorized participants to access hot and cold blockchains, ensuring secure separation and sharing of investigation, identity information, and digital evidence videos. The blockchain records are immutable, improving transparency and reliability. Experimental results show performance impacts related to storage capacity and transmission rates, indicating the system's effectiveness in handling large files. Future work will focus on network peer effects, improving transaction speeds, and reducing code complexity, aiming to strengthen the management of digital evidence in Korea.
14. Rao, S., et al (2020). In this paper, a new system for digital evidence management is proposed which utilizes Blockchain technology. Blockchain by its pattern applies the concepts of integrity, transparency, security, authenticity, and auditability. This makes it one of the best choices for the maintenance and tracing back of the forensic chain of custody. The digital evidence will be handled by this system that has been proposed from the time it is retrieved until it is presented as evidence in the court. It will guarantee integrity, traceability, authenticity and security of the evidence. It will also help guarantee that this digital evidence gets admissible in the Court of Law.
15. Jeong, J., et al (2020). The paper on the "Design and Implementation of a Digital Evidence Management Model Based on Hyperledger Fabric" outlines a system for securely storing and managing digital evidence using a permissioned blockchain. Evidence is timestamped and linked to unique cryptographic identifiers, with smart contracts automating management tasks to ensure transparency and accountability. Hyperledger Fabric’s privacy and permission features allow controlled access based on roles. This approach offers enhanced security, immutability, and scalability. However, challenges include the need for specialized blockchain knowledge and consideration of implementation and maintenance costs for successful adoption.
16. Wright, S (2020). This paper states integration of blockchain technology into the criminal justice system. It is crucial for enhancing evidence integrity and restoring public trust. This cost-effective solution enables law enforcement agencies to continue using their existing products while minimizing human error and criminal intent. Alister Inc. and LOCARD.EU aim to implement blockchain for evidence tracking, allowing for immutable records of evidence from crime scenes to court. By registering only hashes that represent the physical evidence state, the system facilitates faster processing and better storage. Ultimately, this approach can help reduce wrongful arrests and convictions, highlighting the urgent need for reform within the justice system. Implementing blockchain is essential to ensure accurate evidence management and maintain due process worldwide.
17. Yunianto, E., et al (2019). The design of the DEC (Digital Evidence Management) concept using blockchain technology (BDEC) involves translating DEC requirements into a structured data type, with smart contracts facilitating data storage on the blockchain. This framework ensures the secure management of digital evidence by accommodating minimum storage needs. Adjustments are necessary for data processing, including the ability to handle various file types and integrating logging features for evidence tracking. The DEC-based blockchain can also integrate with digital evidence storage (DES), enhancing security through software solutions like encryption. Additionally, the framework's implementation can be adapted for different data types requiring integrity, and it can be applied to other blockchain platforms that support smart contracts.
18. Gopalan, S. H., et al (2019). This paper emphasizes the advantages of blockchain technology in maintaining and securing the chain of custody (CoC) in digital forensics. By leveraging features such as security, integrity, transparency, and auditability, blockchain emerges as the optimal solution for CoC in the digital era. Its distributed nature prevents unauthorized alterations, thereby reducing conflicts and enhancing trust among users. The study presents a thorough examination of blockchain's application in digital forensics and proposes a method to provide these services to the forensic community.
19. Bonomi, S., et al (2018). The administration of proof is quite possibly of the main test in advanced legal sciences. From the time they are gathered until they are utilized in an official courtroom, different members in the examination can see the proof, and they take brief responsibility for. Even though various organizations control the proof, this strategy, known as Chain of Custody (CoC), should guarantee that it doesn't change during the examination for it to be acknowledged in a court. Computerized confirmations of CoC are presently totally constrained the hard way, and associations in the chain are expected to finish up going with documentation. To guarantee auditable proof honesty and proprietor recognizability while dematerializing the CoC cycle, we propose a Blockchain-based Chain of Custody (B-CoC) technique in this work. We tried the exhibition of an Ethereum-based B-CoC model.

**REFERENCES**

1. Alqahtany, S. S., & Syed, T. A. (2024). ForensicTransMonitor: A Comprehensive Blockchain Approach to Reinvent Digital Forensics and Evidence Management. *Information*, *15*(2), 109.
2. Yao, Q., Xu, K., Li, T., Zhou, Y., & Wang, M. (2024). A secure image evidence management framework using multi-bits watermark and blockchain in IoT environments. *Wireless Networks*, *30*(6), 5157-5169.
3. Miller, A., & Singh, A. (2024, March). Chain of Custody and Evidence Integrity Verification Using Blockchain Technology. In *International Conference on Cyber Warfare and Security* (Vol. 19, No. 1, pp. 168-176).
4. Dhulavvagol, P. M., Totad, S. G., & Anagal, A. (2024). SHARD-FEMF: adaptive forensic evidence management framework using blockchain sharding and IPFS. *Int. Arab J. Inf. Technol.*, *21*(2), 179-190.
5. Santos, N. M. B. R. D. (2024). *Multiparty trust levels in evidence management: Ensuring tamper-proof chain of custody in blockchain* ( Master’s thesis).
6. Batista, D., Mangeth, A. L., Frajhof, I., Alves, P. H., Nasser, R., Robichez, G., ... & Miranda, F. P. D. (2023). Exploring blockchain technology for chain of custody control in physical evidence: A systematic literature review. *Journal of Risk and Financial Management*, *16*(8), 360.
7. Shivani, E., Vidyadhari, G., Reddy, D., & Unnisa, R (2023). An Implementation Of Blockchain Technology In Forensic Evidence Management.
8. Rana, S. K., Rana, A. K., Rana, S. K., Sharma, V., Lilhore, U. K., Khalaf, O. I., & Galletta, A. (2023). Decentralized model to protect digital evidence via smart contracts using layer 2 polygon blockchain. *IEEE Access*, *11*, 83289-83300.
9. Chougule, H., Dhadiwal, S., Lokhande, M., Naikade, R., & Patil, R. (2022). Digital evidence management system for cybercrime investigation using proxy re-encryption and blockchain. *Procedia Computer Science*, *215*, 71-77.
10. Akhtar, M. S., & Feng, T. (2022). Using blockchain to ensure the integrity of digital forensic evidence in an iot environment. *EAI Endorsed Transactions on Creative Technologies*, *9*(31), e2-e2.
11. Borse, Y., Patole, D., Chawhan, G., Kukreja, G., Parekh, H., & Jain, R. (2021, May). Advantages of blockchain in digital forensic evidence management. In *Proceedings of the 4th International Conference on Advances in Science & Technology (ICAST2021)*.
12. Tsai, F. C. (2021). The application of blockchain of custody in criminal investigation process. *Procedia Computer Science*, *192*, 2779-2788.
13. Kim, D., Ihm, S. Y., & Son, Y. (2021). Two-level blockchain system for digital crime evidence management. *Sensors*, *21*(9), 3051.
14. Rao, S., Fernandes, S., Raorane, S., & Syed, S. (2020, June). A novel approach for digital evidence management using blockchain. In *Proceedings of the International Conference on Recent Advances in Computational Techniques (IC-RACT)*.
15. Jeong, J., Kim, D., Lee, B., & Son, Y. (2020). Design and implementation of a digital evidence management model based on hyperledger fabric. *Journal of Information Processing Systems*, *16*(4), 760-773.
16. Wright, S (2020). The Use of Blockchain within Evidence Management Systems.
17. Yunianto, E., Prayudi, Y., & Sugiantoro, B. (2019). B-DEC: Digital evidence cabinet based on blockchain for evidence management. *Int. J. Comput. Appl*, *181*(45), 22-29.
18. Gopalan, S. H., Suba, S. A., Ashmithashree, C., Gayathri, A., & Andrews, V. J. (2019). Digital forensics using blockchain. *International Journal of Recent Technology and Engineering*, *8*(2), 182-184.
19. Bonomi, S., Casini, M., & Ciccotelli, C. (2018). B-coc: A blockchain-based chain of custody for evidences management in digital forensics. *arXiv preprint arXiv:1807.10359*.