**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).

In conclusion, our research marks a pivotal advancement in computer forensics by introducing a generic framework that leverages blockchain technology to embed forensic transactions, enhancing data integrity, authenticity, and transparency throughout the forensic investigation process. By making each forensic action an immutable entry on the blockchain, our approach significantly elevates the standards of reliability and verifiability in the field. The integration of smart contracts offers a seamless interface for forensic activities, ensuring each step in the investigation is recorded in a tamper-proof and transparent manner, which is crucial for legal proceedings. Our empirical evaluation underscored the efficiency and practicality of using smart contracts, highlighting minimal latency and operational overhead. This framework not only bolsters the credibility of forensic evidence in legal contexts but also serves as a versatile model for a broad range of forensic applications, from IoT to cloud computing, contributing profoundly to the integrity of judicial processes and the broader pursuit of justice.

1. Yao, Q., et al (2024).

In this work, we present a novel image evidence protection framework in the image forensics scenario based on digital image watermarking and blockchain technology. First, a multi-bit digital image watermarking algorithm has been proposed, which can embed the watermark signals containing additional event information related to the image. In addition, the proposed image watermarking algorithm is based on self-supervised learning algorithm, which means that the watermarked image is more robust against to geometric and noise attacks than the traditional image watermarking models with fixed transform basis. Furthermore, because the watermark signal stored in the smart contract includes the event information corresponding to the image, when the watermarked image (as the image evidence) is provided to the image forensic experts or other users, both the image and its corresponding event information can be authenticated after checking and verifying the watermark extracted from the image with the watermark stored in the smart contract. Finally, the experimental results have demonstrate the feasibility and efficacy of the proposed framework. Albeit our proposed framework can be viewed as a first step to the image evidence protection, further reducing the distortion of watermarked image as well as extending to the video evidence preservation are important issues that warrant further study. In addition, for multi-bits watermarking algorithms, the limitation of the payload size is not only related to the number of pixels in the image, but, more important, also to the content of the image. So, it is difficult to provide an accurate limitation of the payload size according to the number of pixels of an image, especially for self-supervised learning-based image watermarking models. Therefore, our future study also includes the exploration of the limitation of the payload size of our proposed watermarking algorithm according to the given image.

1. Miller, A., et al (2024).

This study introduces an innovative model designed to ensure the integrity and preservation of digital evidence and the chain of custody, ultimately increasing the likelihood of digital evidence being deemed admissible in a court of law. The foundation of this model relies on blockchain and smart contract technology, where IntegriStore comes into play. IntegriStore incorporates smart contract-driven role-based access control, eliminating the constraint of a single owner per piece of evidence. This, in turn, fosters improved collaboration among team members during digital forensic investigations. Furthermore, by entrusting access control to the smart contract, the logging of the chain of custody becomes guaranteed. What is particularly advantageous is that the system can read the blockchain state directly from indexed events, allowing for seamless integration with external subsystems without burdening the blockchain with additional overhead. The web interface offers users direct interaction with both the blockchain and the storage engine, simplifying the overall experience. However, a notable limitation of this model pertains to the potential complexity and size of the smart contract, which may present challenges in terms of management and navigation. For future work, it is recommended that efforts be directed toward creating a more streamlined, smart contract structure. This would help optimize the management of the blockchain while maintaining the effectiveness of the model. A proof of concept has been developed to showcase IntegriStore's feasibility and its ability to preserve the chain of custody, providing a strong foundation for future refinements and expansion of the model. Future research could explore ways to make the model more scalable and adaptable to different use cases, potentially offering a valuable tool for the digital forensic investigators’ community.

1. Dhulavvagol, P. M., et al (2024).

The SHARD-FEMF framework represents a significant advancement in the field of forensic evidence management. Through a comprehensive evaluation and analysis, we can draw several key conclusions about the framework’s effectiveness and potential. Firstly, SHARD-FEMF has demonstrated its ability to significantly enhance the efficiency of forensic evidence management. It achieves this by reducing gas consumption by an average of 21.5%, indicating improved computational efficiency and resource optimization. This reduction in gas consumption ensures not only cost-effectiveness but also improved performance in handling forensic evidence. Secondly, the framework has exhibited remarkable improvements in time consumption, reducing it by 40%. This efficiency gain results in quicker processing and management of evidence, which is crucial in forensic investigations where time plays a critical role. Additionally, SHARD-FEMF showcases improved scalability, allowing for a 23% increase in transaction scalability without compromising performance. This scalability is essential in handling a growing volume of forensic evidence efficiently. Overall SHARD-FEMF is a promising solution for the efficient and secure management of forensic evidence. Its ability to reduce gas consumption, improve time efficiency, enhance scalability, and provide robust security features makes it a valuable asset in the realm of forensic investigations. This framework has the potential to revolutionize the way forensic evidence is handled, ultimately aiding law enforcement agencies and the justice.

1. Santos, N. M. B. R. D. (2024).

In a time where International Criminal Justice is assuming center stage once again, it is relevant and urgent to equip its institutions with tools and mechanisms that could help them further their mandate of bringing justice within the scope of their mandate. For the International Criminal Court, it is to bring an end to impunity, and justice and reparations to its victims. The DSRM approach was adopted, and as such, the six stages of this approach were considered, which were divided within this dissertation in four major work packages. The first stage – Problem identification and motivation; was fulfilled with the identification of the added value of blockchain technology within the area of evidence management and chain of custody within the sector. This was evaluated and validated using the Blue Ocean Strategy methodology. The second stage – solution objectives; of the solution was enabled and enriched with the literature review, which provided valuable insights of what was found in the body of knowledge. The third and fourth stages – design, development, and demonstration; are covered and depicted in the MultiTrustBloc framework. The fifth stage – evaluation; leveraged a panel of experts in this area within the sector of international criminal justice, providing a validation of the usefulness of such solution. The sixth and final stage – Communication; validated the novelty of this dissertation by having its core contributions materialized in the approval of two papers in the conference IBICA 2023.

1. Batista, D., et al (2023).

This research conducted a comprehensive literature review on the utilization of blockchain technology to ensure control and maintenance of the chain of custody of physical evidence. The analysis demonstrated that there is a lack of research regarding the use of blockchain technology and smart contracts to improve reliability and ensure the integrity of the physical evidence chain of custody. It must be noted that the chain of custody requirements need to be general enough to understand how solutions can be applied to both digital and physical evidence chains of custody. Therefore, an important conclusion of this work is that there is a clear research opportunity regarding the use of blockchain technology in the chain of custody of physical evidence. Since the integrity and trustworthiness of the evidence in the chain of custody are important to avoid future litigation, the use of blockchain technology is ripe for such a context. It can mitigate legal risks, as well as facilitate compliance and auditing. These features can be reinforced by the proposal of a blockchain framework in the chain of custody, which allows for data availability, and, thus, frictionless access to data.

In terms of management, the results of this study demonstrate that not only digital forensics could benefit from blockchain tools to guarantee the trustworthiness of the evidence chain of custody but also traditional forensics. An example of the beneficial aspect of blockchain is that its immutability feature increases the security of chain of custody recording. Also, blockchain allows for a complete visualization of all the registries of evidence made through the chain of custody life cycle in a more linear and organized manner. Another contribution of blockchain to the forensics field would be of economic nature. Since evidence chain of custody maintenance has a public interest and is primarily a government responsibility, using blockchain as a platform to guarantee the recording and integrity of the chain of custody could decrease government expenditures in public safety and judicial proceedings.

Through a comprehensive analysis of existing literature, this systematic review has unveiled significant prospects and notable shortcomings in utilizing blockchain technology in the chain of custody. These findings highlight the potential benefits various domains can derive from harnessing blockchain. The review has brought to light many opportunities for industries to explore through research and development initiatives, specifically by integrating blockchain into the chain of custody framework. These opportunities extend beyond criminal investigations, encompassing diverse sectors such as Oil & Gas.

Furthermore, future research work involves an in-depth discussion for ensuring control and preserving the chain of custody of physical evidence, analysis of the limitations of the proposed blockchain solutions to mitigate existing risks related to the chain of custody, and research regarding existing problems in the control of the physical evidence chain of custody.

1. Shivani, E., et al (2023).

From the moment evidence is obtained from the scene of the crime until a decision is made by a court, it is essential to preserve its integrity. It is essential to preserve the chain of custody because it may demonstrate whether the evidence was tampered with during the process of collecting and processing it. The digitalization of the chain of custody through the application of Blockchain technology guarantees the security, validity, and integrity of forensic data exchanges. Not only will the use of blockchain make it better for the environment, but it will also improve security thanks to encryption, which can only be viewed remotely by authorized individuals. The chain of custody procedure will be carried out by an algorithm that will make use of blockchain technology, specifically Hyperledger Fabric.

1. Mehta, S., et al 2023).
2. Rana, S. K., et al (2023).

In this paper, we presented a decentralized model for protecting digital evidence using smart contracts on the Layer 2 Polygon blockchain. Our strategy takes advantage of the immutability, transparency, and decentralisation features of blockchain technology to guarantee the security and integrity of digital evidence. We create a trustless, automated system using smart contracts that does away with the need for middlemen and lowers the possibility of tampering or manipulation. We showed that our decentralised model is effective and efficient through our experimental evaluation. Real-world applications can benefit from the deployment of the Layer 2 Polygon blockchain because it enables scalable and affordable storage and verification of digital evidence. We make sure the evidence is intact and verifiable throughout its lifecycle by utilising the security characteristics of smart contracts. There are still a few areas, though, that need improvement and more research. The scalability of blockchain technology is one of the major issues since the amount of storage needed for digital proof can soon rise to a significant level. For vast volumes of evidence to be handled effectively in the future, storage and retrieval procedures should be optimised. The incorporation of cutting-edge cryptographic methods to improve the confidentiality and privacy of digital evidence represents another area for future study. Techniques such as zero-knowledge proofs or homomorphic encryption can be explored to enable secure computations on encrypted evidence without revealing sensitive information. Furthermore, the usability and accessibility of the system should be improved to encourage widespread adoption. User-friendly interfaces and seamless integration with existing digital forensic tools can help bridge the gap between traditional forensic workflows and decentralized systems. Lastly, the legal and regulatory aspects surrounding the use of decentralized systems for handling digital evidence need to be addressed. Collaboration with legal experts and policymakers is crucial to ensure compliance with existing laws and regulations and to establish a legal framework that accommodates the unique features and challenges of decentralized systems.

1. Chougule, H., et al (2022).

The main outcome of this work is a prototype of a software system that uses the access control paradigm to access data stored in unsaturated environments. For the implementation purpose of the algorithms for the system, acceptable, functionality, and implementation complexity were chosen. Customization of access policiesin order to define dynamic access policies; changing access policies requires no extra action from some another members of a social system, eliminating the need for frequent changes to user keys; the integrity of information about all transactions, including granting and changing access, facts improves. A blockchain-based system with configurable data encryption permission is proposed

1. Akhtar, M. S., et al (2022).

Digital forensics is a branch of forensics that is concerned with the investigation of digital evidence. Digital forensics is concerned with the detection, acquisition, processing, analysis, and reporting of material that has been saved in an electronic format. When it comes to law enforcement investigations, digital forensics assistance is essential because electronic evidence can be found in nearly all instances of unlawful behavior. It is feasible to discover what information has been taken and how it has been duplicated or disseminated by using digital forensics techniques. It is possible that some hackers will purposely destroy data in order to cause harm to their targets. In other cases, malicious software or hacker activity might cause crucial data tobe corrupted without the user's knowledge.One of the difficulties that digital forensics must deal with is the threat to security and integrity. It is possible for IoT devices to collect digital forensic evidence in an IoT environment, which may pose a significant risk for cybercrime agencies due to concerns about security and integrity of the data collected. The integrity and security of Internet of Things (IoT) based digital forensics have recently been the subject of numerous studies, but confidentiality is the most significant issue that researchers are dealing with. Recent research and related investigations demonstrated that tampering and security-related issues continue to persist in digital forensics, despite advances in technology. Consequently, asmart and effective model is necessary that not only maintains security and integrity, but also predicts threats in advance to aid the system in its operation. We are presenting a system that is both intelligent and effective, which makes use of Blockchain technology in conjunction with the Hashing algorithm. Following the acquisition of crime evidence through Internet of Things devices, the data will be stored in a Blockchain. During that time period, we will be employing Machine Learning boosted models in order to predict anomalies in the evidence and transactions. The proposed model is effective as a result of its ability to detect and forecast attacks on an early enough basis. The XGBoost algorithm was used to forecast an early time attack, which was successful. Figure 1 illustrates the performance of XGBoost in terms of early attack detection in order to maintain system security and integrity. XGBoost has demonstrated accuracy in terms of early attack detection in orders data, accounts data, and transactional data of 99.8%, 95%, and 79 percent, respectively for the early prediction of attacks in the three different types of data. Meanwhile, KMEANS has demonstrated the accuracy of confidence clustering with 98 percent, 58 percent, and 59 percent for each data set, according to the results.

1. Borse, Y., et al (2021).

The field of Digital Forensic is extending and there is a vast difference in management of Digital Evidences as compared to Physical Evidence management, traditionally presented in the Court of Law. Blockchain Technology has the potential to provide the features crucial in digital evidence management. Blockchain can be configured to provide authority, authenticity, integrity, transparency, auditability, and security. Therefore, Blockchain Technology has the advantage for keeping up, maintaining and following the forensic and scientific chain of custody over conventional methods. There is a great chance of decrease in conflict through expanded trust with blockchain and blockchain surely brings a genuine guarantee for the Forensic Network and Community in this manner. Hence, to avoid the manual errors to affect the admissibility of digital evidence in court of law, blockchain technology can be considered as a viable solution to maintain chain of custody of digital evidence.

1. Tsai, F. C. (2021).

With the emerging technology trend, the dramatic increase of digital evidence has a great impact on criminal investigation. Since digital evidence is vulnerable in nature, how to maintain the integrity and authenticity of digital evidence become a crucial task. In this study, we propose a blockchain of custody framework which supports evidence collection and transferring in a lawful manner. In order to distinguish different level of authorization to access sensitive crime cases, we design the role of investigator to encompass various criminal investigation actions. The combinations of creator and owner with the role of investigator make evidence collecting and transferring more rigorous and ensure the integrity and authenticity of digital evidence during the entire judicial process. The framework is implemented on Ethereum blockchain with smart contract. The experimental results show that the proposed model can validate the immutability of evidence data and facilitate crime case sharing more effectively. Future research directions may include exploring more roles involved in criminal investigation and considering the scalability issue when deploying the proposed framework in a wider range of applications.

1. Kim, D., et al (2021).

The digital crime evidence data obtained during the investigation of a criminal case is transmitted and managed on a physical hard disk until it is analyzed and submitted to the court, and there is a risk that it can be damaged or manipulated by an attack. Therefore, digital crime evidence videos that were difficult to obtain and analyze are not adopted as court evidence, because the continuity of storage cannot be guaranteed. Criminal evidence data are not modified once stored, but investigation information is frequently modified. In this paper, we proposed a two-level blockchain system to increase the integrity of digital crime evidence, so as to efficiently manage criminal evidence. In the proposed system, only authorized participants can access the hot and cold blockchains, in a decentralized environment to separate, store, and share the original information of the investigation, identity information, and digital crime evidence videos. The two-level blockchain system stores the investigation and identity information, as well as digital crime evidence videos, by on-site investigators with verified identities. In addition, by separating data into two blockchains, the same transaction can be stored in the ledgers of all institutions participating in the channel, and the same block can be generated by executing a smart contract. Investigation and identity information, as well as digital crime evidence videos, once created in blocks, cannot be deleted by any user. In addition, because the block is shared with all institutions in the two-level blockchain system, transparency and reliability are enhanced.

We also evaluated the performance of the proposed system. According to the experimental results, when the storage performance of the cold blockchain increased from 100 MB to 1 GB in units of 100 MB, the average performance decreased by 0.11 TPS. In addition, it was confirmed that when the capacity increased by 1 GB from 1 GB to 5 GB, the decrease was 0.7 TPS on average. The query performance of the cold blockchain had an average decrease of 1.4 TPS when increasing in steps of 100 MB, from 100 MB to 1 GB, and an average decrease of 6.8 TPS when increasing in steps of 1 GB.

In addition, the experimental results of the hot blockchain revealed that the storage function decreased the TPS by 3.82 when the transmission rate increased from 100 TPS to 500 TPS in units of 100 TPS, and the inquiry performance increased by 79.8 TPS. This is the difference according to the capacity width of the digital crime evidence video used in the experiment, and the transmission rate of the identity and investigation information, and it was confirmed that the actual uniform capacity and the TPS according to the increase in transmission rate were predictable.

The proposed system is suitable for a system that can search while storing data with large files for recording, and ensure the integrity of the data. It can be applied to other applications considering data with similar characteristics, but there is a limitation in applying it to various applications in general. Additionally, for the two-level blockchain system to be used as an actual digital evidence management system, further performance improvements will be required. To this end, as future work, we must first perform an experiment to show the effect of the number of peers in the network. We also intend to research a two-level blockchain system that can respond to high transaction transmission speeds. We also plan to lower the code complexity within the cold blockchain. In the future, it is expected that the proposed two-level blockchain system will contribute to lowering the threat that exists in the transmission and management of digital evidence in Korea, and increasing reliability as a result.

1. 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.

1. Jeong, J., et al (2020).

For the conventional linear array MIMO radar, the reverse projection method is unable to correctly locate multi-targets with different distances because of the coupling of distance and angle in near-field. The structure of symmetric sub-array is designed, and the received signals of two sub-arrays are jointly reconstructed in this paper. The reconstructed signals can realize the distance-independent DOA estimation, and the subsurface target localizations are obtained with different distances. On this basis, the grid zooming design of spatial segmentation is used to optimize the localization efficiency. The effectiveness of the proposed localization method and optimization schemes is verified by simulation results.

1. Wright, S (2020).

In conclusion, the use of blockchain to enhance the integrity of evidence in the criminal justice system is vitally important and just makes sense. It can be an inexpensive and comprehensive solution allowing agencies to continue using all of their existing products while removing most elements of human error and criminal intent from the process. Alister Inc. and LOCARD.EU plan to implement blockchain in the chain of evidence to help restore the public trust in the criminal justice system. Through blockchain, the verified tracking of evidence within different law enforcement agencies will be possible. Only hashes proving the physical evidence “state” will be registered within the system allowing for better and faster processing and more digital storage space. The attribution of hashes to physical pieces of evidence will allow for immutable tracking of evidence from scene to court, and this system will allow for inadmissible evidence to be easily dismissed in a timely manner. Through the unfortunate cases that have been described above, the authors and researchers from Alister Inc. hope to give their readers a firm grasp of the importance blockchain will have within the justice system, and the many ways it will support the fight toward a more just and accurate criminal evidence tracking system. Accurate evidence with proven integrity is critical in maintaining due process within the judicial system worldwide, and using blockchain to track it can help decrease the instances of political turmoil due to false arrests and convictions. If we fail to correct this systemic problem within our criminal justice system, we will all suffer the loss of many hard-working, honest, and falsely accused Americans who might have been an excellent Police Officer, or the next great Doctor, Lawyer, Researcher, or Inventor. We simply can’t afford not to change, and blockchain in the supply chain of evidence is the change we need to implement.

1. Yunianto, E., et al (2019).

The design of DEC concept with blockchain technology (BDEC) was carried out by translating DEC requirements into a struct data type. Smart contract is responsible for applying DEC on the blockchain when storing data. It has obtained a digital evidence management design. It must accomodate the minimum needs of digital evidence data by storing it safely on the blockchain. The DEC framework can be built on the blockchain. Some adjustments are needed in the data processing section. One of them is designing a framework development to be able to accommodate a variety of digital data consisting of many files (split files). In addition, some adjustments made are adding the logging concept that accompanies digital evidence. Furthermore, the framework was developed by integrating with the storage location of evidence. It can be concluded if the DEC-based blockchain can be developed up to integration with digital evidence storage (DES). Later the system must be able to secure digital evidence in a software manner. That it needs to increase the level of security of digital evidence even further such as the use of encryption etc. The same implementation can be done in various types of data that require data integrity such as sending confidential documents etc. Of course, by adjusting needs, especially on smart contracts. The same system can be implemented on other types of blockchain outside of ethereum on the condition that the blockchain is used instead of supporting smart contracts.

1. Gopalan, S. H., et al (2019).

Blockchain by proposal harvests the best of security, integrity, transparency and audit thus making it the unsurpassed choice for maintaining and securing the forensicCoC. Blockchain decreases conflict and increases belief through the distributed blockchain making it impossible to alter every block. Blockchain is the most effective solution for CoC for the digital era of forensics. This paper presented on Digital Forensics in Blockchain: We provide a detailed study of the blockchain using CoCand the proposed method of providing the service to the forensics community for their use.

1. Bonomi, S., et al (2018).

This paper presented B-CoC, a blockchain-based architecture to dematerialise the CoC process in digital forensics. We also provided a prototype of the B-CoCarchitecture based on the Geth implementation of Ethereum nodes. Based on the performance evaluation, B-CoC showed to be an effective support for the CoC process as it is able to sustain realistic workload with an acceptable overhead in terms of memory used to store the chain. The current implementation assumes that the set of validators node is fixed and that validators are available to sacrifice their privacy when participating in the consensus process. As a future work, we are investigating how it is possible to manage a dynamic set of validators and most important we are studying alternatives that allow to increase the level of privacy for validators not altering other dependability and security attributes.

**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. Mehta, S., Kumari, K. S., Jain, P., Raikwar, H., & Gore, S. (2023, March). Blockchain driven evidence management system. In *2023 3rd International conference on Artificial Intelligence and Signal Processing (AISP)* (pp. 1-6). IEEE.
9. 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.
10. 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.
11. 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.
12. 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)*.
13. Tsai, F. C. (2021). The application of blockchain of custody in criminal investigation process. *Procedia Computer Science*, *192*, 2779-2788.
14. Kim, D., Ihm, S. Y., & Son, Y. (2021). Two-level blockchain system for digital crime evidence management. *Sensors*, *21*(9), 3051.
15. 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)*.
16. 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.
17. Wright, S (2020). The Use of Blockchain within Evidence Management Systems.
18. 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.
19. 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.
20. 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*.