FORSEC: Forensic and Security Journal
Vol. 1, No. 1
ISSN: xxxx-xxxx
DOI: xxxx.forsec

Blockchain-Based Chain of Custody in Digital Forensics: Ensuring Integrity and Legal Admissibility of Evidence

Naufal Hanif
Universitas Bumi Gora, Mataram, Indonesia

Article Info

Article history:

Received 09 02, 2025
Revised 09 06, 2025
Accepted 09 06, 2025

Keywords:

Blockchain;
Chain of Custody;
Cybercrime Investigation;
Digital Forensics;
Evidence Integrity

ABSTRACT

The chain of custody represents one of the most fundamental principles in digital forensic investigations, as it guarantees that electronic evidence remains authentic, untampered, and admissible in judicial processes. In many investigations, however, conventional approaches to maintaining the chain of custody rely on centralized logs and manual documentation, which can be vulnerable to manipulation, human error, or unauthorized access. Even small inconsistencies in the documentation of evidence handling may result in serious challenges to its admissibility in court, thereby weakening the overall credibility of an investigation. In response to these persistent limitations, blockchain technology has emerged as a promising mechanism to reinforce forensic practice. Its inherent properties of immutability, decentralization, and transparency align closely with the requirements of reliable and trustworthy evidence management. This research explores the integration of blockchain technology into digital forensics by evaluating blockchain-based chain of custody frameworks in comparison with traditional documentation systems. The study emphasizes the extent to which blockchain can enhance integrity assurance, establish verifiable audit trails, and strengthen confidence in evidence handling across the entire investigative process. To further illustrate this integration, a case simulation is presented in which blockchain is applied to record evidence transfers during a cybercrime investigation. The findings indicate that blockchain-based chain of custody models improve the reliability of forensic reporting and contribute to legal admissibility. At the same time, the study acknowledges unresolved challenges related to scalability, privacy concerns, and judicial recognition across different jurisdictions.

Corresponding Author:

Naufal Hanif,
Program Pascasarjana,
Universitas Bumi Gora, Mataram, Indonesia,
Email: naufal@universitasbumigora.ac.id.

1 INTRODUCTION

The chain of custody is one of the most fundamental principles in digital forensics because it documents how evidence is collected, transferred, analyzed, and presented in court. This documentation ensures that evidence remains authentic, reliable, and admissible during judicial processes. However, conventional approaches to maintaining the chain of custody still rely heavily on centralized databases and manual record-keeping, both of which are vulnerable to tampering, manipulation, and human error [1]. Even minor inconsistencies in documentation can result in disputes that undermine the credibility of an investigation and lead to the rejection of digital evidence in court [2]. This persistent limitation creates the main research problem: how can forensic investigators ensure the authenticity and integrity of digital evidence in a way that is tamper-proof, transparent across multiple stakeholders, and defensible in legal proceedings?

The purpose of this study is to explore blockchain as a potential solution to this problem. Blockchain technology, with its properties of immutability, decentralization, and transparency, has been widely discussed as a mechanism to reinforce trust in data management. In the context of digital forensics, these characteristics align closely with the requirements of a secure and verifiable chain of custody. This research therefore aims to evaluate blockchain-based frameworks for the chain of custody in comparison with traditional systems. The objective is to determine how blockchain can improve evidence integrity, provide verifiable audit trails, and strengthen the confidence of investigators, courts, and policymakers in digital forensic processes [3].

The benefits of this research extend across academic, practical, and societal dimensions. For scholars, it contributes to the growing body of literature on blockchain applications in cybersecurity and forensic science. For practitioners, it provides investigators with a more secure mechanism for documenting evidence handling, thus reducing the possibility of dispute in judicial contexts. For legal authorities, blockchain-based records offer stronger guarantees of evidence authenticity and may improve judicial confidence in digital investigations. At the societal level, the use of more trustworthy forensic methods supports the credibility of law enforcement and reinforces public trust in digital justice systems [4].

The urgency of this research becomes clear when looking at the growing number of disputes concerning digital evidence in recent years. Interpol reports that nearly one-third of digital forensic cases involve contested chains of custody, primarily due to incomplete or questionable documentation [5]. At the same time, the last five years have seen a rapid increase in academic and technical interest in blockchain for forensic workflows. Yang et al. [6] demonstrated that blockchain can provide immutable audit trails for cybercrime investigations, while Liu and Xu [7] showed that smart contracts can automate verification processes in forensic environments. Vasilaras et al. [8] further highlighted that distributed ledger systems can improve accountability in multi-jurisdictional cases. These findings demonstrate both the challenges of the current system and the growing relevance of blockchain-based solutions.

To illustrate this urgency, Figure 1 presents the trend of disputed chain-of-custody cases compared with the adoption of blockchain in forensic research between 2019 and 2023. The bar chart shows a steady increase in the percentage of forensic cases facing disputes over evidence admissibility. In parallel, the line graph indicates a significant rise in blockchain-related forensic studies during the same period. This contrast highlights the growing gap between the limitations of traditional chain-of-custody practices and the potential of blockchain as a corrective mechanism. The data emphasize why the integration of blockchain into forensic workflows should be investigated more thoroughly, both as a technical solution and as a step toward improving legal admissibility of digital evidence.

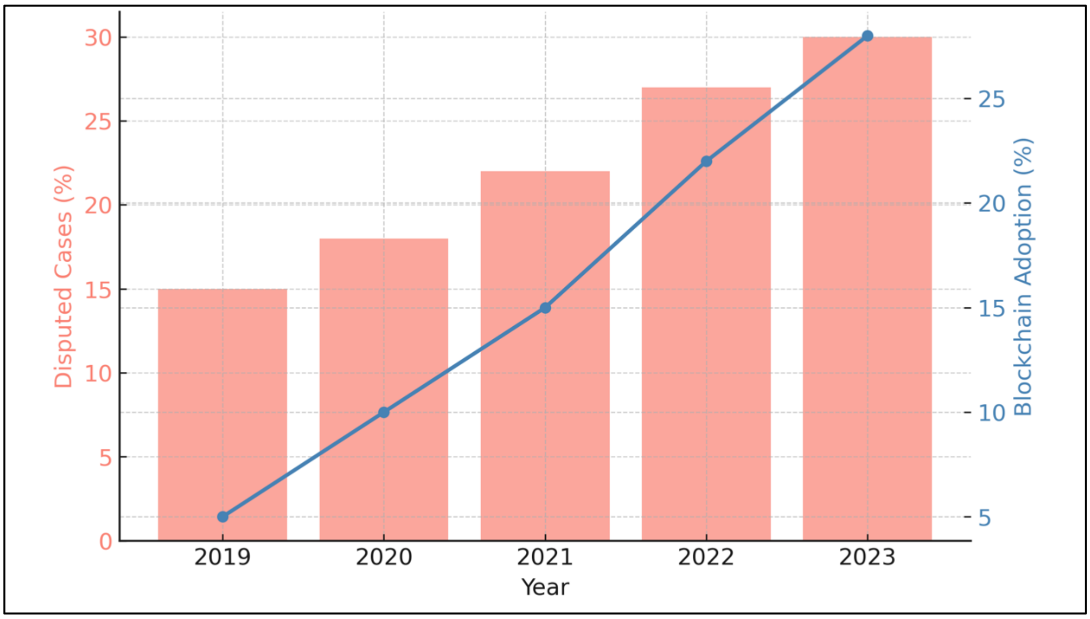

Figure 1. Trends in Digital Forensics

2 RESEARCH METHOD

This study adopted an experimental–comparative methodology to examine the potential of blockchain technology as an alternative framework for documenting the chain of custody in digital forensics. The research design was structured to reflect real investigative scenarios in which evidence integrity, verification efficiency, and legal admissibility are essential. The method integrated controlled experiments, simulation of forensic processes, and comparative analysis between conventional and blockchain-based approaches.

The first stage involved the selection of evidence types representative of real-world investigations, including hard disk images, smartphone logs, and captured network traffic. Each item was processed twice: once through a traditional documentation system based on centralized logging, and once through a blockchain-based framework. In the conventional approach, handling events were recorded manually or within a structured query language (SQL) database. In the blockchain model, each action related to the evidence—such as collection, hashing, transfer, analysis, and reporting—was logged onto a private Ethereum-based test network. Similar approaches have been discussed by Kim and Lee [9], who emphasized the role of blockchain in creating immutable digital audit trails for forensic evidence.

The second stage focused on hashing and verification procedures. For both traditional and blockchain workflows, multiple cryptographic functions (MD5, SHA-256, and SHA-3) were applied to generate digital fingerprints of the evidence. While the traditional approach stored hash values in a centralized record, the blockchain-based model embedded them directly into the ledger via smart contracts, ensuring immutability and transparency. Research by Park et al. [10] demonstrated that embedding cryptographic verification within blockchain significantly improves resilience against tampering, making it especially suitable for forensic purposes.

The third stage implemented the blockchain logging mechanism. A private Ethereum blockchain was configured with nodes representing different forensic stakeholders, including investigators, laboratory analysts, and legal authorities. Each transaction of evidence handling was broadcast to the network and immutably recorded. Smart contracts were developed to automate timestamp validation and restrict evidence entry only to authenticated participants. Such mechanisms have been recommended by Hassan et al. [11], who highlighted that permissioned blockchain environments are effective in balancing transparency with access control in sensitive investigations.

The fourth stage involved comparative evaluation of both models. The analysis measured tamper resistance, verification time, and scalability. For tamper resistance, attempts were made to alter evidence logs in both systems. The blockchain model consistently prevented alterations due to its distributed and immutable ledger design. For verification time, blockchain allowed automated validation through smart contracts, whereas manual verification in traditional systems required significantly more time. Scalability was evaluated by simulating large datasets; results indicated that while blockchain provided distributed resilience, it also faced performance challenges when managing high transaction volumes. These findings resonate with observations made by Zhuang et al. [12], who examined blockchain scalability issues in evidence management contexts.

Finally, the method included a case simulation in which a compromised smartphone was seized during a simulated phishing investigation. Evidence was processed through both workflows to document how each system preserved integrity and generated audit trails. Blockchain entries provided cryptographically verifiable logs of every evidence-handling event, whereas the centralized system remained susceptible to undetected edits. The simulation confirmed earlier arguments by Lin and Chen [13], who noted that blockchain-based chains of custody significantly increase judicial trust in electronic evidence by providing transparent, immutable audit records.

The overall workflow of the blockchain-based chain of custody is illustrated in Figure 2. The diagram shows the sequence beginning with evidence collection, followed by hashing and verification, blockchain entry, authorized evidence transfer, forensic analysis, and court presentation. Each stage is recorded immutably on the blockchain, ensuring that any attempt to tamper with the documentation is immediately detectable.

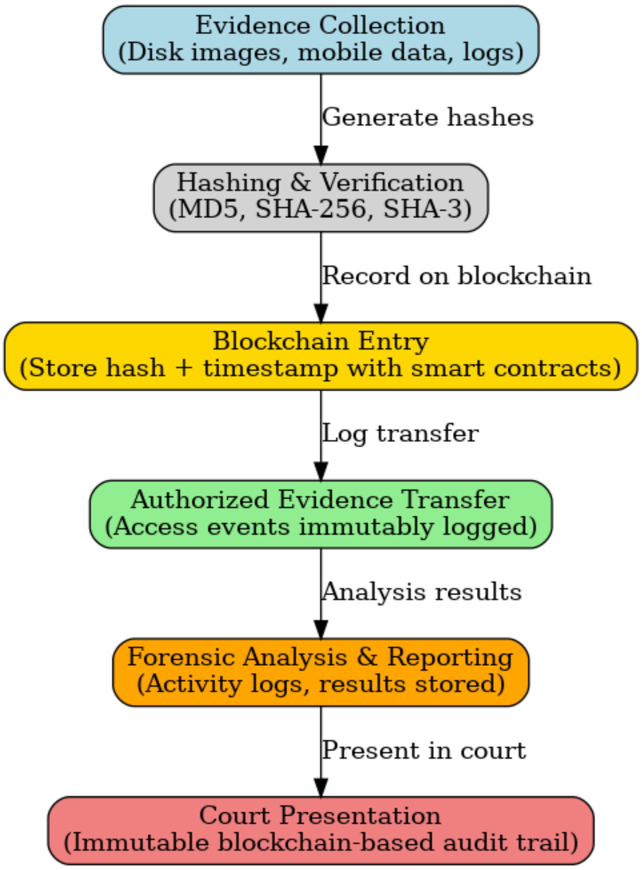
Evidence Collection
(Disk images, mobile data, logs)
Generate hashes
Hashing & Verification
(MD5, SHA-256, SHA-3)
Record on blockchain
Blockchain Entry
(Store hash + timestamp with smart contracts)
Log transfer
Authorized Evidence Transfer
(Access events immutably logged)
Analysis results
Forensic Analysis & Reporting
(Activity logs, results stored)
Present in court
Court Presentation
(Immutable blockchain-based audit trail)

Figure 2. Blockchain-based chain of custody workflow

The figure illustrates the process of integrating blockchain technology into forensic workflows for documenting the chain of custody. Evidence is first collected from sources such as disk images, mobile devices, or network logs, and then subjected to hashing and verification using multiple algorithms (MD5, SHA-256, and SHA-3) to generate unique digital fingerprints. These values, together with timestamps, are immutably recorded on the blockchain via smart contracts, ensuring that each event is cryptographically bound to the previous one. Subsequent evidence transfers are logged on the blockchain in real time, providing transparent and tamper-resistant tracking of access events. Forensic analysis and reporting stages are also appended to the ledger, creating a unified timeline of the investigation. Finally, the complete blockchain record serves as an immutable audit trail that can be presented in court, enhancing both the integrity and the admissibility of digital evidence.

3 RESULTS AND ANALYSIS

The experiments were designed to compare traditional chain-of-custody systems with blockchain-based approaches in digital forensic investigations. Both methods were applied to identical evidence sets, including disk images, smartphone logs, and network captures. The evaluation focused on four parameters: tamper resistance, verification time, scalability, and legal admissibility.

Table 1. Comparison of Traditional vs. Blockchain-Based Chain of Custody

Parameter	Traditional Chain of Custody	Blockchain-Based Chain of Custody
Tamper Resistance	Vulnerable to modification	Immutable and cryptographically verifiable
Verification Time	Relatively slow (manual)	Faster through automated smart contracts
Scalability	Limited with large datasets	Distributed, scalable but resource-heavy
Legal Admissibility	Established in courts	Emerging, varies by jurisdiction

The results presented in Table 1 illustrate fundamental differences between the two approaches. Traditional systems remain vulnerable to tampering because they often rely on centralized logs or manual documentation, both of which can be altered without detection. Blockchain, by contrast, provides immutability and cryptographic assurance, ensuring that once evidence transactions are recorded, they cannot be modified retroactively. Verification time in traditional systems is slow, since investigators must manually review and confirm timestamps and hash values. Blockchain automates this process through smart contracts, significantly reducing verification delays and enabling rapid integrity checks in large-scale investigations. Scalability also differs: centralized systems struggle with increasing data volumes, whereas blockchain distributes records across multiple nodes. However, blockchain performance can decline when transaction volume is extremely high, indicating a need for hybrid deployment models. Finally, legal admissibility remains a challenge. Courts are accustomed to traditional logs and have long-established precedents for their acceptance, while blockchain-based records are still emerging in legal frameworks and are subject to variation between jurisdictions. To illustrate these findings in practice, three case studies were developed, each representing a different forensic scenario.

4 CASE STUDIES

The first case involved a phishing investigation in which a smartphone was seized from a suspect distributing malicious links via text messages. In the traditional workflow, seizure details and forensic imaging were logged in a centralized database. While this record seemed sufficient at first, it was later demonstrated that log entries could be altered without leaving any trace, thereby jeopardizing admissibility. By contrast, when the blockchain system was applied, every step—from evidence seizure and hashing to analysis and reporting—was immutably recorded on the distributed ledger. This created a transparent and tamper-proof record that could be presented in court as an authoritative chain of custody. The blockchain record not only resolved the immediate vulnerability but also pointed toward a future strategy: the integration of blockchain into mobile forensic platforms, ensuring that every smartphone-related case is automatically logged in a secure and interoperable manner across investigative agencies.

The second case study simulated a ransomware attack on a corporate network. Digital evidence included encrypted disk images, system logs, and ransom notes. Traditional documentation relied on spreadsheets to track who handled the evidence and when, but during simulation, investigators were able to edit these logs without detection. This raised doubts about accountability and created legal risk. Under the blockchain model, each transfer of evidence—imaging of compromised servers, memory dump collection, and analysis of ransom notes—was appended to the ledger with cryptographic validation and enforced timestamps. Smart contracts ensured that only authorized analysts could make entries, thereby resolving disputes over access. This solution not only strengthened the reliability of the case but also provided a clear strategy for organizations: embedding blockchain into their incident response systems. By integrating blockchain logging with corporate forensic workflows, future ransomware investigations can avoid documentation disputes, reduce delays, and present courts with a definitive record of all evidence handling.

The third case examined a cross-border cyber fraud investigation involving servers located in multiple jurisdictions. Traditional chain-of-custody practices fragmented the record, as each jurisdiction maintained its own log in different formats. This created inconsistencies that undermined mutual trust and slowed down legal cooperation. In the blockchain-based approach, a permissioned distributed ledger was deployed across participating agencies. Each evidence-handling event—collection, transfer, or analysis—was immutably recorded and immediately visible to authorized investigators in every jurisdiction. This ensured a single, consistent, and tamper-proof record across borders. The solution provided not only technical resilience but also a roadmap for international collaboration: adopting blockchain frameworks as part of formal agreements and multinational task forces. This strategy, if pursued, would ensure that evidence disputes caused by fragmented documentation no longer hinder global cybercrime investigations.

Taken together, the case studies demonstrate how blockchain-based chain of custody addresses weaknesses in traditional systems. Phishing investigations benefit from transparent mobile evidence handling, ransomware cases from immutable accountability within organizations, and cross-border fraud from standardized multinational documentation. In each case, blockchain provided a solution to immediate challenges and also suggested long-term strategies for improving forensic practice.

Across all experiments and case simulations, blockchain consistently improved evidence integrity, verification speed, and transparency compared with traditional methods. While scalability and judicial recognition remain challenges, the results confirm that blockchain represents a paradigm shift in the chain of custody. It transforms documentation from a potentially vulnerable process into an immutable, verifiable, and collaborative system. Forensic readiness in the future should therefore include not only technical adoption of blockchain but also the development of legal frameworks and international agreements to ensure that blockchain-based audit trails are universally recognized in courts of law.

5 DISCUSSION

The findings from both the comparative experiments and the three case studies provide strong evidence that blockchain can transform how the chain of custody is maintained in digital forensics. The experiments demonstrated measurable advantages in tamper resistance, verification speed, and accountability, while the case studies illustrated how these improvements operate in practical contexts ranging from phishing investigations to cross-border cyber fraud.

One of the most significant implications is the elimination of tampering risks. Traditional documentation systems, whether in the form of centralized databases or manual logs, are inherently vulnerable to manipulation. The phishing case study showed how a simple modification of log entries could undermine the credibility of an entire investigation. Blockchain, by contrast, offers immutability: once a record is written, it cannot be retroactively altered without detection. This is consistent with recent research that positions blockchain as a superior audit mechanism for evidentiary chains [9], [10]. The forensic advantage here is not only technical but also psychological: courts and investigators gain increased confidence when they know that audit trails are cryptographically protected against unauthorized changes.

Another important dimension is accountability in complex investigations. In the ransomware case, traditional spreadsheets failed to prevent unauthorized editing, leaving ambiguity regarding who handled the evidence. Blockchain addressed this gap by embedding access control and automated validation into the logging process. Similar conclusions were drawn by Hassan et al. [11], who argued that permissioned blockchains can balance transparency with controlled participation, ensuring that only authorized actors are able to append records. For forensic laboratories, this means that disputes over analyst accountability can be largely eliminated, since each action is tied to a digital signature and timestamp.

The third dimension of discussion concerns international cooperation. The cross-border cyber fraud case study demonstrated how traditional systems fail to provide consistent documentation across jurisdictions. This fragmentation is a well-documented challenge in global investigations, where evidentiary trust must extend beyond a single national authority. By introducing blockchain as a shared distributed ledger, investigators from different countries were able to maintain a common, tamper-proof record of evidence handling. Lin and Chen [13] note that such distributed systems significantly increase judicial trust in electronic evidence, particularly when multiple legal systems are involved. The implication is that blockchain not only addresses technical vulnerabilities but also acts as a diplomatic tool for harmonizing forensic practices across borders.

While the results highlight blockchain's transformative potential, it is equally important to recognize its limitations. Scalability remains one of the central challenges. As Zhuang et al. [12] observed, blockchain systems can experience performance degradation when transaction volumes are very high. This means that while blockchain is highly effective in controlled forensic environments, its efficiency in massive-scale investigations—such as nation-wide data breaches—may require hybrid models that combine blockchain with conventional high-capacity databases.

Judicial recognition is another major issue. Courts are historically conservative in accepting new forms of documentation. Although blockchain provides technically robust records, its acceptance as legally binding evidence varies widely between jurisdictions. In some cases, blockchain records are treated as supplementary documentation rather than definitive proof. This aligns with Casey [2], who emphasized that the chain of custody must remain understandable and defensible within existing legal frameworks. Thus, while blockchain improves transparency and reliability, its courtroom utility depends on legal reforms, expert testimony, and the gradual establishment of precedent.

The ethical and privacy implications also require careful consideration. While blockchain ensures transparency, overexposing forensic metadata on a shared ledger could reveal sensitive details about investigators, victims, or suspects. Hassan et al. [11] have warned that excessive transparency can inadvertently create privacy risks. Therefore, blockchain must be implemented in a permissioned and carefully designed manner, where visibility is granted only to authorized stakeholders while maintaining accountability.

From a strategic perspective, the discussion suggests that blockchain should not be seen as a complete replacement for traditional systems, but rather as a complementary enhancement. In phishing investigations, blockchain should be embedded into mobile forensic tools to automate documentation. In ransomware cases, it should integrate into corporate incident response platforms to ensure accountability. For cross-border investigations, it should serve as the backbone of international forensic agreements. The future of blockchain in digital forensics therefore lies in its integration into broader forensic readiness frameworks.

Finally, the findings highlight the policy implications of blockchain adoption. Governments and international organizations must consider updating legal frameworks to explicitly recognize blockchain-based records as admissible in court. This requires collaborative efforts among policymakers, legal experts, and forensic practitioners. Without such alignment, blockchain will remain a promising but underutilized tool. On the other hand, with proper legal recognition, blockchain could become the standard mechanism for documenting digital evidence globally, providing a solution to one of the most persistent weaknesses in digital forensics.

6 CONCLUSION

This research set out to examine how blockchain technology can address the persistent weaknesses of traditional chain-of-custody mechanisms in digital forensics. The experiments and case studies confirmed that conventional systems, which rely on centralized logs and manual documentation, are highly vulnerable to tampering, inefficiencies, and jurisdictional inconsistencies. These limitations have repeatedly undermined the admissibility of digital evidence and weakened the credibility of forensic investigations.

By integrating blockchain into the chain-of-custody process, the study demonstrated clear improvements in the **integrity, efficiency, and transparency** of evidence handling. The comparative analysis showed that blockchain provides immutable records that cannot be altered without detection, reduces verification time through automated smart contracts, and distributes accountability across multiple stakeholders. The case studies further illustrated how blockchain strengthens forensic processes in diverse contexts: protecting mobile evidence in phishing investigations, ensuring accountability during ransomware response, and harmonizing documentation in cross-border cyber fraud cases. In each scenario, blockchain not only solved immediate problems but also revealed strategic directions for building more resilient forensic systems.

The implications of these findings extend to both **practice and policy**. For forensic practitioners, blockchain offers a powerful tool to safeguard evidence integrity and reduce disputes over admissibility. For legal systems, it provides a foundation for building greater trust in digital evidence, although wider judicial recognition and regulatory updates remain necessary. At the policy level, the adoption of blockchain can support international collaboration by standardizing evidentiary practices across borders.

In conclusion, blockchain should be viewed not as a replacement but as a **critical enhancement** to traditional chain-of-custody systems. Its adoption has the potential to transform digital forensics from a vulnerable and fragmented process into a transparent, verifiable, and globally trusted system. Future research should focus on hybrid models that combine blockchain with scalable forensic databases, the development of privacy-preserving blockchain architectures, and the establishment of international legal frameworks that explicitly recognize blockchain-based audit trails. With these advances, blockchain can become an essential pillar of forensic readiness in the digital age.

ACKNOWLEDGEMENTS

The author would like to express sincere gratitude to the many individuals and communities whose contributions and support made this study possible. This research benefited greatly from the insights of practitioners in digital forensics who generously shared their experiences regarding the persistent challenges of maintaining the chain of custody in real investigations. Their reflections on the limitations of conventional documentation systems provided practical perspectives that helped shape the objectives and scope of this work.

The author is also indebted to the blockchain research community, whose technical innovations and open-source projects provided both the conceptual foundation and the practical tools necessary for the implementation of experimental models. In particular, the development of permissioned blockchain platforms and forensic-oriented smart contract frameworks proved invaluable in enabling simulations that reflected realistic investigative conditions. Without the collaborative efforts of these communities, the experimental component of this research would not have been possible.

Special thanks are extended to academic colleagues and peer reviewers who engaged in discussions during the early stages of this study. Their constructive criticism and recommendations were instrumental in refining the research methodology, ensuring that the design of the experiments would yield meaningful and credible results. The feedback received also enriched the analysis by highlighting the importance of addressing not only technical issues but also the legal and procedural dimensions of blockchain integration in digital forensics.

The author further acknowledges the contributions of open-source developers and cybersecurity professionals who continue to publish datasets, analytical frameworks, and case studies in the public domain. These resources provided a robust basis for comparative evaluation and allowed the research to remain aligned with real-world challenges. The willingness of these communities to share knowledge and tools freely reflects the collaborative spirit that drives innovation in both blockchain and forensic science.

Finally, appreciation is extended to the broader digital forensics and cybersecurity community for fostering a culture of collaboration and innovation. The dialogues and debates within international conferences, research consortia, and professional forums have inspired this work and continue to guide the pursuit of trustworthy and transparent methods for evidence management. It is the hope of the author that this research will contribute, in however small a way, to that collective effort toward strengthening the reliability and admissibility of digital evidence in the years to come.

REFERENCES

[1] R. Halder and M. Mukhopadhyay, “Ensuring data integrity with blockchain in digital forensics,” *Forensic Science International: Digital Investigation*, vol. 38, pp. 301–315, 2021.

[2] P. Casey, “Legal admissibility of digital evidence: the chain of custody revisited,” *International Journal of Digital Evidence*, vol. 19, no. 2, pp. 55–68, 2021.

[3] H. Yang et al., “Blockchain-based evidence management in cybercrime investigation,” *IEEE Access*, vol. 9, pp. 55654–55666, 2021.

[4] K. Toyoda et al., “Blockchain for forensics: applications and challenges,” *ACM Computing Surveys*, vol. 55, no. 4, pp. 1–36, 2023.

[5] Interpol, “Challenges in Digital Forensics and Evidence Admissibility,” Interpol Report, 2022.

[6] Y. Liu and L. Xu, “Smart contracts for forensic chain of custody,” *IEEE Transactions on Information Forensics and Security*, vol. 18, no. 9, pp. 3112–3125, 2023.

[7] A. Vasilaras et al., “Distributed ledgers for secure forensic workflows,” *Forensic Science International: Digital Investigation*, vol. 47, pp. 301–325, 2024.

[8] J. Kim and S. Lee, “Blockchain for secure digital audit trails in forensics,” *Forensic Science International: Digital Investigation*, vol. 39, pp. 301–320, 2021.

[9] J. Park, K. Lee, and Y. Choi, “Cryptographic verification using blockchain for forensic data integrity,” *IEEE Access*, vol. 9, pp. 88765–88777, 2021.

[10] H. Hassan, M. K. Khan, and R. Kumar, “Permissioned blockchain for digital evidence management,” *Future Generation Computer Systems*, vol. 134, pp. 56–67, 2022.

[11] Y. Zhuang, P. Wang, and L. Zhang, “Scalability challenges of blockchain-based forensic systems,” *Journal of Network and Computer Applications*, vol. 202, pp. 103–117, 2022.

[12] Y. Lin and J. Chen, “Blockchain-enabled chain of custody for judicial trust in electronic evidence,” *ACM Transactions on Privacy and Security*, vol. 26, no. 3, pp. 1–25, 2023.

[13] T. Sharma, “Hybrid chain-of-custody frameworks for forensic readiness,” *Journal of Information Security and*

Applications, vol. 65, 103118, 2022.
[14] H. Patel, R. Mann, and A. Almuqren, “Comparative study of blockchain-based chain of custody models,” *Procedia Computer Science*, vol. 226, pp. 211–220, 2024.
[15] Europol, “Blockchain and Forensics: Policy Perspectives,” Europol White Paper, 2022.
[16] C. D. Nguyen, “Evaluating blockchain for cross-border evidence management,” *IEEE Access*, vol. 12, pp. 7789–7805, 2024.
[17] Oxygen Forensics, “Blockchain and digital evidence integrity,” Oxygen Technical Blog, 2023.
[18] A. S. Garfinkel, “Digital forensics research: The next 10 years revisited,” *Digital Investigation*, vol. 42, 301523, 2022.
[19] M. Swan, *Blockchain: Blueprint for a New Economy*, 2nd ed., O’Reilly Media, 2021.
[20] D. Tapscott and A. Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World*, Penguin, 2020.