An Analysis of Blockchain Solutions for Digital Evidence Chain of Custody

Irene Lavín[1] and Diego R. Llanos[1]

Computer Science, Universidad de Valladolid, Spain.
{irene.lavin,diego.llanos}@uva.es

Abstract. Chain of custody (CoC) preservation is essential to ensure the integrity and authenticity of digital evidence in legal and forensic settings. This review article examines how Blockchain-based solutions address the requirements of ISO 27037, which regulates the identification, collection, acquisition and preservation of digital evidence. An initial taxonomy is also proposed to classify blockchain-based solutions. The analysis reveals significant shortcomings in aspects such as auditability, scalability and legal admissibility. Finally, key recommendations are presented to strengthen the integration between Blockchain and ISO 27037 guidelines, fostering more robust solutions aligned with international forensic standards.

Keywords: ISO 27037 · CoC · Blockchain.

1 Introduction

In an increasingly digital world, preserving the chain of custody of digital assets is crucial to ensure data integrity and provenance. This review article aims to explore existing solutions based on Blockchain technology to improve the chain of custody of digital assets and analyse, focusing on the ISO 27037 standard [7], whether these solutions integrate the standard. This would provide a comprehensive understanding of the current state of the art, identify the strengths and limitations of existing approaches, and guide future research and development in this field.

The ISO 27037 standard, which provides guidelines for the handling of digital evidence, can be strengthened by Blockchain technology. The decentralized, immutable and transparent nature of Blockchain allows for automatic data preservation, creating a secure and auditable chain of custody [8]. Previous research such as Forensic-Chain [9] and B-DEC [16] has demonstrated the potential of Blockchain-based solutions to improve digital evidence management. Furthermore, the application of Blockchain in personal data management highlights its ability to improve auditability and transparency in data collection, retention and exchange [10].

To expand on this topic, it is proposed to develop a taxonomic framework to classify and analyse the various blockchain-based solutions for preserving the chain of custody of digital assets. This would provide a comprehensive understanding of the current state of the art, identify the strengths and limitations of existing approaches, and guide future research and development in this field.

2 Analysis of ISO 27037 Standard

The ISO 27037 standard provides a comprehensive framework for the management of digital evidence, encompassing identification, collection, acquisition, and preservation [14]. It details the essential steps to ensure the integrity and admissibility of digital evidence in legal proceedings, highlighting the documentation of the chain of custody.

Specifically, the standard emphasizes the importance of maintaining a clear and uninterrupted chain of custody, which involves documenting the possession, handling, and control of digital evidence from its initial identification to its final disposition [15]. This process is crucial to establish authenticity and trustworthiness by demonstrating that the evidence has not been tampered with or altered during the investigation. The standard also addresses secure storage, preservation of the original state of the evidence [12], and the maintenance of detailed records throughout the entire chain of custody [1].

2.1 Purpose and Scope

The ISO 27037 standard serves as a guide for organizations and individuals involved in the handling of digital evidence, such as law enforcement agencies, forensic investigators, and information security professionals.

The three main objectives of the standard [7] are:

1. Identification, collection, acquisition, and preservation of digital evidence.
2. Ensuring evidence integrity for legal, disciplinary, or investigative actions.
3. Facilitating the exchange of digital evidence between jurisdictions.

It applies to various devices, including computers, hard drives, mobile phones, and networked systems. Digital still and video cameras, navigation systems, and similar devices.

2.2 Key Principles

The ISO 27037 standard highlights several key principles [7] that are essential in preserving the chain of custody for digital evidence.

- Relevance: Evidence must be directly related to the investigation.
- Reliability: Processes must ensure the evidence is what it claims to be.
- Sufficiency: Adequate evidence must be collected to support the investigation.

Additionally, the standard emphasizes the importance of maintaining the original state of the evidence, preventing contamination, and ensuring strict handling procedures.

Table 1. Key aspects and their relationship with the processes of digital evidence handling.

	Auditability	**Justifiability**	**Repeatability**	**Reproducibility**
Identification	×	×		
Collection	×	×	×	
Acquisition	×	×	×	×
Preservation	×	×	×	×

2.3 Digital Evidence Handling

Key aspects of Digital Evidence Handling Several key aspects that are crucial to the effective handling of digital evidence are underscored by the ISO 27037 standard [7]. These core elements, as outlined in the standard, include:

- Auditability: A complete and transparent record of all actions taken with the digital evidence, allowing independent verification of the process.
- Justifiability: A clear rationale for all decisions and actions taken during the evidence handling process.
- Repeatability: The ability to obtain the same results when the same process is followed by a different person using the same tools and methods under the same conditions.
- Reproducibility: The ability to obtain the same results when the same process is followed by a different person using different tools and methods under different conditions.

Processes for Digital Evidence Handling The ISO 27037 standard outlines a series of processes for handling digital evidence [7]. These processes are critical in establishing the integrity and traceability of digital evidence, which is essential for it to be admissible in legal proceedings. The methods are described below.

1. Identification: Recognise and document potential digital evidence, prioritising collection based on data volatility to avoid loss.
2. Collection: Convey digital evidence-containing devices to secure facilities for examination. Comprehensively document all undertaken actions.
3. Acquisition: Create verified copies of digital evidence using approved methods.
4. Preservation: Evidence must be protected from tampering, environmental hazards, and accidental damage. It should be stored in secure facilities with access controls and monitoring.

Table 1 wants to show how the four key aspects of the handling of digital evidence (auditability, justifiability, repeatability, and reproducibility) are related to each process of the mentioned evidence handling.

Justifiability, auditability, repeatability, and reproducibility are crucial for preserving the integrity of digital evidence throughout the entire handling process (identification, collection, acquisition, and preservation), as established by

Table 2. Summary of responsibilities deduced from the roles of ISO 27037.

- **Digital Evidence First Responder (DEFR)**
  - Securing the scene: Protecting the location and devices from unauthorised access.
  - Identifying potential evidence: Recognising devices that may contain relevant digital information.
  - Documenting the initial state: Taking notes, photos, etc. before touching any evidence.
  - Preventing data alteration: Avoiding actions that could modify data.
  - Reporting findings to authorities or specialists.
- **Digital Evidence Specialist (DES)**
  - Identification of relevant digital evidence.
  - Collection of physical devices and media in a forensically sound manner.
  - Acquisition of forensic copies to ensure integrity and prevent alteration.
  - Preservation of digital evidence throughout its lifecycle, including storage and CoC.
  - Meticulous documentation of all actions to maintain auditability and CoC.
  - Compliance with legal and organizational requirements.
- **Digital Evidence Custodian (DEC)**
  - Maintaining chain of custody: Documenting all evidence handlers, transfer dates, and reasons.
  - Secure storage: Protecting evidence from unauthorized access, damage, or degradation.
  - Controlled access: Restricting who can access evidence, with access records.
  - Proper handling: Transferring evidence per procedures and documenting in chain of custody.
- **Legal Authority (LA)**
  - Initiating the investigation and the need for digital evidence.
  - Defining the investigation scope and required digital evidence.
  - Providing legal authorization for evidence collection and acquisition.
  - Receiving reports and findings from digital evidence examination.
  - Ensuring the legal and ethical conduct of the investigation.
- **Forensic Facility Management (FFM)**
  - Aligning procedures with ISO 27037.
  - Ensuring staff are trained and competent in digital evidence handling.
  - Providing necessary tools and resources for digital forensics work.
  - Overseeing QA/QC processes in the lab.
  - Managing workflow and resources for digital investigations.

the ISO 27037 standard. The Digital Evidence First Responder (DEFR) must justify and document all actions, from evidence selection to preservation methods. Maintaining a clear audit trail is essential, and processes must be repeatable to ensure consistency and, where applicable, reproducible across different tools or methods. This ensures the reliability and legal admissibility of digital evidence.

Table 3. Summary of Blockchain-based solutions, indicating coverage of the ISO 27037 standard and detected areas for improvement (Part One).

1. *B-CoC: A Blockchain-Based Chain of Custody for Evidence Management in Digital Forensics* [5]
   Coverage: This paper proposes a Blockchain-based system to dematerialize the CoC process, ensuring the integrity and traceability of the collected evidence.
   Areas for Improvement:
   - There is limited discussion on integrating Blockchain solutions with existing ISO standards.
   - It does not provide a comprehensive taxonomy of Blockchain-based CoC solutions.
   - It lacks exploration of legal admissibility and cross-jurisdictional challenges.
2. *A Survey on Blockchain-Based IoT Forensic Evidence Preservation* [11]
   Coverage: This survey examines the role of Blockchain in preserving forensic evidence within IoT environments, addressing challenges such as evidence integrity and authenticity.
   Areas for Improvement:
   - It focuses primarily on IoT contexts, with less emphasis on broader digital asset CoC.
   - It does not analyse ISO norms or establish a detailed taxonomy of Blockchain solutions.
   - There is limited discussion on the auditability of collected hashes.
3. *Exploring Blockchain Technology for Chain of Custody Control in Physical and Digital Evidence* [4]
   Coverage: Through a systematic literature review, this paper analyses Blockchain-based solutions for CoC issues applicable to both physical and digital evidence.
   Areas for Improvement:
   - It does not delve deeply into ISO 27037 analysis.
   - It lacks a structured taxonomy of Blockchain-based CoC solutions.
   - There is minimal focus on the auditability aspects of collected hashes.
4. *Blockchain to ensure integrity and traceability in the chain of custody of digital evidence* [13]
   Coverage: This research classifies Blockchain characteristics that ensure the integrity and traceability of digital evidence in the CoC process based on a systematic mapping study.
   Areas for Improvement:
   - Limited analysis of ISO norms.
   - It does not provide a comprehensive taxonomy of Blockchain solutions.
   - It lacks discussion on the auditability of collected hashes.
5. *ForensiBlock: A Provenance-Driven Blockchain Framework for Data Forensics and Auditability* [2]
   Coverage: A Blockchain framework that automates investigation steps, ensures secure data access, traces data origins, preserves records, and expedites provenance extraction.
   Areas for Improvement:
   - It does not analyse the ISO 27037 standard or related standards.
   - It lacks a detailed taxonomy of Blockchain-based CoC solutions.
   - It focuses more on provenance and auditability than on the entire CoC process.
6. *B-DEC: Digital Evidence Cabinet based on Blockchain for Evidence Management* [16]
   Coverage: It provides a secure and auditable system for recording evidence details, access logs, and chain of custody information.
   Areas for Improvement:
   - It does not demonstrate compliance with the four key aspects of digital evidence handling.
   - Focused on the technical implementation of B-DEC, without relying on ISO 27037.
   - Limited details on how the auditability and integrity of the recorded hashes are ensured.

2.4 Ensuring accuracy and integrity of Digital Evidence

The ISO 27037 standard [7] emphasizes the importance of maintaining the accuracy and integrity of digital evidence throughout the entire investigation process. This ensures that the copy of the evidence is correct and has not been tampered with. A combination of technical and procedural safeguards is as follows.

1. Use of Verification Functions: Emphasizes the importance of demonstrating that evidence hasn't been modified.

Table 4. Summary of Blockchain-based solutions indicating coverage of the ISO 27037 standard and detected areas for improvement (Part Two).

7. *Blockchain Forensics: A Systematic Literature Review of Techniques, Applications, Challenges, and Future Directions* [3]
   Coverage: It provides a broad overview of Blockchain forensics, covering techniques, applications, and key forensic challenges related to data integrity, authenticity, and non-repudiation.
   Areas for Improvement:
   - It lacks a discussion on how Blockchain forensics aligns with the requirements of the ISO.
   - Does not provide a mapping between the discussed techniques and sections of the ISO.
   - Does not discuss practical implementation. Focus on technical aspects of Blockchain.
8. *A Data Preservation Method Based on Blockchain and Multidimensional Hash for Digital Forensics* [8]
   Coverage: The method uses Blockchain and multidimensional hashing to ensure data integrity.
   Areas for Improvement:
   - Lacks explicit reference and alignment with the ISO 27037 standard.
   - Limited analysis of how the method integrates with the general processes of the ISO.
   - Insufficient details on the practical implementation and scalability of the proposed method.
   - Legal implications and the admissibility of Blockchain-based evidence in courts are not described.
9. *Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer* [9]
   Coverage: It aims to create a secure and tamper-proof record of evidence handling, demonstrating a practical implementation with a Proof of Concept using Hyperledger Composer.
   Areas for Improvement:
   - Not based on the standard and lacks a clear demonstration of how it meets its requirements.
   - It focuses on a specific use case. Does not address integration with other forensic processes.
   - Does not discuss legal implications of using Blockchain-based evidence, particularly regarding its admissibility in courts.
10. *Blockchain Based Digital Evidence Chain of Custody* [14]
    Coverage: It creates a tamper-proof and transparent record of evidence handling. It incorporates timestamping mechanisms to provide verifiable records of evidence acquisition and handling.
    Areas for Improvement:
    - Lacks a clear demonstration of how it meets the requirements of the standard.
    - Does not provide sufficient details on the practical implementation and scalability.
    - Does not discuss the legal implications of using Blockchain-based evidence.
11. *Blockchain-based chain of custody* [1]
    Coverage: Blockchain enhances the reliability of the chain of custody by providing a tamper-proof, transparent, and auditable record of digital evidence handling.
    Areas for Improvement:
    - Lacks a clear demonstration of how the solution meets the requirements of the standard.
    - Does not provide details on practical implementation and scalability.
    - Does not discuss the legal implications of using Blockchain-based evidence or how the solution integrates with existing forensic processes and tools.
12. *SoK: Blockchain Solutions for Forensics* [6]
    Coverage: It examines various Blockchain solutions for forensics, including their potential to improve the chain of custody.
    Areas for Improvement:
    - Does not propose a specific solution.
    - Does not directly address the requirements of the ISO 27037 standard or implementation details.

2. Chain of Custody: Details the requirements for maintaining a chain of custody record.
3. Repeatability and Reproducibility: Mentions that all processes should be *auditable and repeatable* and their results *reproducible*.

4. Minimal Intrusion: Acknowledges that preservation cannot always be non-intrusive but stresses the need to minimize changes to the original data.
5. Documentation and Validation: Highlights the need to document all actions and establish a method for verifying the accuracy and reliability of copies compared to the original.
6. Handling Volatile Data: ISO 27037 includes specific guidelines for handling volatile data due to its susceptibility to loss.
7. Use of Trusted Tools and Write Blockers: The use of write blockers is implied in the emphasis on minimizing changes to original data.
8. Logging and Audit Trails: Mentions the importance of *auditing and justification.*

2.5 Roles and Responsibilities

ISO 27037 [7] only mentions as such two main roles, the Digital Evidence First Responder (DEFR) and the Digital Evidence Specialist (DES). However, it implicitly defines several key roles. These roles, Digital Evidence Custodian (DEC), Legal Authority (LA) and Forensic Facility Management (FFM), emerge from the activities described within the standard.

Table 2 shows a summary of responsibilities deduced for each role described above.

2.6 Competency and Training

The standard [7] emphasizes the importance of proper training and certification for all personnel involved in the digital evidence-handling process. Competency requirements are defined for each of the key roles, ensuring that individuals have the necessary skills and knowledge to fulfill their responsibilities while maintaining the integrity of the evidence.

2.7 Additional Guidelines

This section of the ISO 27037 standard [7] provides supplementary guidance on crucial aspects of digital evidence handling, emphasizing proper documentation, effective briefing and adherence to legal compliance requirements. These additional guidelines provide a more holistic approach to digital evidence management, in line with the principles and requirements of the standard.

3 Blockchain-based Solutions and the ISO 27037 standard: A Taxonomy-Based Evaluation

We will now examine several existing solutions and research related to the application of Blockchain to the treatment of the chain of custody and digital evidence. The objective is to see if they take into account the ISO 27037 standard in their research, as well as to determine to what degree and what are the

Table 5. Initial taxonomy of Blockchain-Based CoC Solutions.

1. **Blockchain Type** – Public – Private – Hybrid/Consortium 2. **Architecture** – Permissioned – Permissionless – Hybrid 3. **Data Storage** – On-chain – Off-chain – Hybrid 4. **Scalability** – Transaction Speed – Data Storage Capacity – Network performance	5. **Consensus Mechanism** – Proof-of-Work – Proof-of-Stake – Other 6. **Application Domain** – Digital forensics – Supply Chain Management – Healthcare – Intellectual Property – Other 7. **Integration Capabilities** – Interoperability with Legacy Systems – Compliance with Standards – API Availability 8. **Level of Integration with ISO 27037** – Full – Partial – No Integration

possible areas for improvement. Tables 3 and 4 show a summary of Blockchain-based solutions, as well as an analysis of the coverage of the ISO 27037 standard and the areas for improvement detected.

Table 5 presents an initial taxonomy for categorizing blockchain-based solutions for chain of custody. This taxonomy classifies blockchain solutions based on key characteristics relevant to their implementation and effectiveness in managing the chain of custody.

4 Summary of Missing Features

Table 6 presents a summary of missing features in the articles under analysis. As can be observed, the areas for improvement are grouped into three blocks: correspondence with ISO 27037, practical implementation and scalability, and legal admissibility and integration. For each of the analysed solutions, the area for improvement has been marked with a cross (×).

Some of the works focus on an analysis and do not provide a solution as such. In these cases, it has been equally reviewed whether they offer coverage of the ISO 27037 standard, whether they detail a possible guide for a future solution, and whether they take into account an analysis regarding legal admissibility.

5 Conclusions

Regarding the areas for improvement concentrated in Table 6, it is observed that none of the analysed solutions establishes a clear correspondence with the

Table 6. Summary of Missing Features in the Analysed Solutions

	Bonomi et al. [5]	*Sakshi et al.* [11]	*Batista et al.* [4]	*Vaca et al.* [13]	*Akbarfam et al.* [2]	*Yunianto et al.* [16]	*Atlam et al.* [3]	*Liu et al.* [8]	*Lone et al.* [9]	*Wenqi et al.* [14]	*Ahmad et al.* [1]	*Dasaklis et al.* [6]
Explicit Correspondence with ISO 27037												
Lack of clear and detailed correspondence with the specific clauses of the standard covered by the solution.	×	×	×	×	×	×	×	×	×	×	×	×
Lack of explicit demonstration of how the four key principles of the standard are met.	×	×	×	×	×	×	×	×	×	×	×	×
Practical Implementation and Scalability												
Insufficient detail on the practical application of the solution.			×				×	×				×
Limited information on the scalability of the solution.			×				×	×		×	×	
Lack of clarity on the performance and effectiveness of the solutions in practice.	×		×	×	×	×	×	×	×	×	×	
Legal Admissibility and Integration												
Insufficient discussion on the legal implications of using Blockchain-based evidence.	×	×		×	×	×	×	×	×	×	×	
Insufficient analysis of how they integrate with legal frameworks and evidentiary procedures.	×	×	×	×	×	×	×	×	×	×	×	×

specific clauses of the ISO 27037 standard, nor do they explicitly demonstrate how to comply with the four key principles of the standard (auditability, justifiability, repeatability and reproducibility). Likewise, 33.3% of the reviewed works do not sufficiently address practical implementation. Nor do they address the scalability of the proposed solutions, with 41.6% omitting crucial aspects such as integration with existing systems, management of large volumes of data and interoperability between different platforms. The lack of clarity on the performance and effectiveness of the solutions in practice has been accounted for in 83.3% of the cases. Finally, the legal admissibility of the evidence stored in Blockchain, a fundamental aspect for its use in legal proceedings, is also scarcely treated in the reviewed literature, only in 16.7% of the cases. These shortcomings represent an obstacle to the widespread adoption of Blockchain technology in the management of the chain of custody of digital evidence.

The proposed taxonomy, described in Table 5, can be used to analyse and classify existing and future blockchain-based chain of custody solutions, facilitating comparison and selection based on specific needs and requirements. As future work, we propose the integration of ISO 27037 requirements with Blockchain capabilities in greater depth with an expanded taxonomy, a granular mapping and a detailed evaluation of legal applicability and system architectures. Additionally, we aim to partner with Blockchain researchers or legal experts to enhance the technical and legal aspects of the taxonomy.

Acknowledgments. This work has been partly funded by the NATASHA project (PID2022-142292NB-I00), from the Spanish Ministry of Science, Innovation and Universities. ChatGPT 4o was used exclusively to improve the readability of this work.

References

1. Ahmad, L., Khanji, S., Iqbal, F., Kamoun, F.: Blockchain-based chain of custody (07 2020)
2. Akbarfam, A.J., Heidaripour, M., Maleki, H., Dorai, G., Agrawal, G.: ForensiBlock: A Provenance-Driven Blockchain Framework for Data Forensics and Auditability (Aug 2023), arXiv:2308.03927 [cs]
3. Atlam, H.F., Ekuri, N., Azad, M.A., Lallie, H.S.: Blockchain Forensics: A Systematic Literature Review of Techniques, Applications, Challenges, and Future Directions. Electronics **13**(17), 3568 (Sep 2024)
4. Batista, D., Mangeth, A.L., Frajhof, I., Alves, P.H., Nasser, R., Robichez, G., Silva, G.M., Miranda, F.P.D.: Exploring Blockchain Technology for Chain of Custody Control in Physical Evidence: A Systematic Literature Review. Journal of Risk and Financial Management **16**(8), 360 (Aug 2023)
5. Bonomi, S., Casini, M., Ciccotelli, C.: B-CoC: A Blockchain-based Chain of Custody for Evidences Management in Digital Forensics. OASIcs, Volume 71, Tokenomics 2019 **71**, 12:1–12:15 (2020), arXiv:1807.10359 [cs]
6. Dasaklis, T.K., Casino, F., Patsakis, C.: SoK: Blockchain Solutions for Forensics, pp. 21–40. Springer International Publishing, Cham (2021)
7. ISO/IEC: ISO/IEC 27037:2012 Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence (2012)
8. Liu, G., He, J., Xuan, X.: A data preservation method based on blockchain and multidimensional hash for digital forensics. Hindawi Publishing Corporation **2021**(1) (01 2021)
9. Lone, A.H., Mir, R.N.: Forensic-chain: Blockchain based digital forensics chain of custody with poc in hyperledger composer. Elsevier BV **28**, 44–55 (01 2019)
10. Masluk, A., Gofman, M.: Protecting personal data with blockchain technology. In: Latifi, S. (ed.) Information Technology - New Generations. pp. 119–125. Springer International Publishing, Cham (2018)
11. Sakshi, Malik, A., Sharma, A.K.: A survey on blockchain based IoT forensic evidence preservation: research trends and current challenges. Multimedia Tools and Applications **83**(14), 42413–42458 (Apr 2024)
12. Sheldon, M.D.: Tracking tangible asset ownership and provenance with blockchain. American Accounting Association **36**(3), 153–175 (04 2022)
13. Vaca, P.A., Dulce Villarreal, E.R.: Blockchain para asegurar la integridad y trazabilidad en la cadena de custodia de evidencia digital en informática forense: un estudio de mapeo sistemático. TecnoLógicas **27**(60), e3049 (Aug 2024)
14. Wenqi, Y., Shen, J., Cao, Z., Dong, X.: Blockchain based digital evidence chain of custody (03 2020)
15. Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., Prakash, E., Jayal, A., Khan, I., Hewage, C., Platts, J.: Cybersecurity, data privacy and blockchain: A review (01 2022)
16. Yunianto, E., Prayudi, Y., Sugiantoro, B.: B-DEC: Digital Evidence Cabinet based on Blockchain for Evidence Management. International Journal of Computer Applications **181**(45), 22–29 (Mar 2019)