DOI: 10.2478/ias2024-0007 • JIAS • 19(3) • 2024 • 80-103

# Multiparty trust levels in evidence management: Ensuring tamper-proof chain of custody in blockchain.

**Nuno Santos[1], Joel Curado[1,3], and Joao C. Ferreira [1,2,4]**

1 ISTAR, ISCTE-Instituto Universitário de Lisboa, 1649-026 Lisboa, Portugal; nuno.mbr.santos@gmail.com (N.S.); joelcurado@gmail.com (J.C.); jcafa@iscte.pt (J.C.F.)
2 Inov Inesc Inovação—Instituto de Novas Tecnologias, 1000-029 Lisbon, Portugal
3 Casperlabs, Seestrasse 5, 6300 Zug Switzerland
4 Molde University College - Specialized University in Logistics, Molde, Norway

**Abstract:** International Criminal Courts (ICCs) are guarantors that justice can be achieved for the most egregious crimes against humanity and that surviving victims of those crimes can live with the assurance that the perpetrators will be held accountable for their actions. Those crimes are complex, sensitive and could be used as a weapon for an intervenient' s own purpose and interests. As such, the credibility of these institutions is often attacked, and it is of critical importance that the process in which they pursue their mandate is rigorous and effective. Evidence sits at the core of the judicial process, and the participants rely on it to be authentic, integer and untampered with to ensure the fairness of the proceedings. Without enforcing powers, these ICCs could rely extensively on evidence provided by other parties to build a strong case from inception to the appeals stage. With the increased digitization of evidence, cyberthreats, size and complexity of evidence, traditional methods of managing the chain of custody are becoming vulnerable to the successful act of challenging the admissibility of evidence. Blockchain could be the answer for strengthening the chain of custody in evidence management, as this technology brings essential characteristics such as timestamping, authentication, immutability and trust among independent parties. This research conceives and designs a blockchainbased framework that maintains a tamperproof chain of custody and multilevel trust in evidence management. It ensures the authenticity and indisputability of evidence in judicial proceedings.

**Keywords:** Blockchain: chain of custody: evidence management; court, judicial; international criminal justice; International Criminal Court

## 1 Introduction

International Courts have a very high level of scrutiny due to their multilateral nature, seemingly high nominal running costs and their involvement in high profile cases that could involve international disputes [1], or try powerful persons for crimes against humanity. These proceedings, in this latter example, are usually public and have a wider audience than the Courtroom actors themselves, leading to wider cultural and societal narratives about the crimes being tried [2].

The success of International Criminal Courts (ICCs), in particular, will be perceived based on the fairness of the trials in charging the accused, and this is highly dependent on the ability of prosecution, defense and the Court's registry in managing evidence properly from collection until disclosure [3].

Every single ICC relies on evidence to ensure the fairness of their decisions and as such, any legal team presenting their evidence will need to ensure it was properly collected, not tampered with during its existence until disclosure and that the chain of custody remained intact.

The motivation behind this research stems from the increasing need to address the challenges and complexities associated with situations and cases where the evidence produced comes from multiple parties, with varying trust levels. Minimizing the risk of invalid evidence due to misuse or processual gaps is very important in guaranteeing a credible and fair judicial system.

In many areas within the international criminal justice system, the use of third parties to acquire and corroborate evidence is widely employed due to the limited resources these organizations have to

perform such actions, which is exacerbated by the lack of enforcement capabilities in their jurisdictions. It is also critical, however, that a third party to an investigation, such as an NGO, a citizen's organization, or a state actor, provide their evidence to be analyzed with the highest standard of duty of care and assurances of the trustworthiness of the evidence.

The need for cooperation with credible third-party actors is further exacerbated with technological advances which allow for the possibility to produce and share evidence in almost real-time, making the person taking that action a very powerful agent of justice. This development has also increased the amount of data that is generated and that requires review, validation, and custody. This increase in quantity and complexity of evidence reinforces the need to identify new ways to protect it well against mishandling or tampering, as it could harm proceedings and be an obstacle to the delivery of justice.

Trust is the cornerstone of justice, and any discrepancies or gaps in the chain of custody can have severe consequences for the involved parties and the overall out-come of a case. To ensure these threats are mitigated but the benefits of the crowdsourcing of justice are realized, it is important to have a solution that can cater to such requirements.

Taking the ICC, headquartered in The Hague, as a basis for this research, it does not prescribe how the process and methods of collecting evidence should be done, rather what the requirements and minimum acceptable thresholds are. Its guiding documents, with respect to evidence procedures, are its founding document, the Rome Statute [4] and the Rules of evidence and procedure document [5].

## *1.1 Problem identification*

Today, trust in public institutions can easily be tarnished, equipping institutions with confidence enhancing mechanisms that can guarantee trust, speed up core processes and increase collaboration are critical for the successful achievements of these institutions.

In the realm of international jurisprudence, the ICC stands as a beacon for prosecuting heinous crimes that resonate on a global scale. A pivotal component of this mandate is the meticulous management and authentication of evidentiary materials, which are frequently procured from a myriad of sources, encompassing national judiciaries, non-governmental organizations and other international entities. These conventional systems, while comprehensive, occasionally grapple with challenges related to ensuring unbroken chains of custody and the inviolability of evidence.

The potential for human oversight, inadvertent errors or deliberate manipulation cannot be entirely discounted. Furthermore, the extant procedures for corroborating the authenticity of third-party evidence can be intricate and protracted, potentially engendering procedural inefficiencies and contestations during legal deliberations. Given this backdrop, a compelling exigency emerges for an innovative, impregnable, and streamlined system dedicated to evidence management and authentication.

## *1.2 Objectives*

Taking into consideration the mentioned issues, the research conducted for this document aims to devise a solution that enables the inviolability of the chain of custody for judicial evidence and leverages on the capacity of credible partners to acquire, validate, and submit potential evidence. The requirements for this solution are based on the ICC's public rules and procedures, however it could be appropriate in many other related organizations.

Another aspect of this study is to explore blockchain technology as the underlying framework for the proposed solution, and how its characteristics of immutability, traceability and tamper-proof, provide an ideal technological foundation to track and manage the evidence from collection to disclosure in trial.

In summary, this research has three main objectives:

1. Validate blockchain as an underlying solution for evidence management and compare it with alternatives.
2. Review and systematize the body of knowledge in blockchain and judicial chain of custody.
3. Design and conceive a Blockchain based system that supports a tamperproof chain of custody during the process of evidence acquisition, usage and disclosure made by independent multiple parties.

## *1.3 Key Concepts*

**The International Criminal Court (ICC):** The ICC is an important institution in the realm of international justice. Established as the world's first permanent ICC, its primary objective is to investigate and, where warranted, prosecute individuals charged with the most severe crimes that

concern the global community. These crimes include genocide, war crimes, crimes against humanity, and the crime of aggression [6].

The ICC was formed under the guidance of an international treaty known as the Rome Statute [4]. Its creation was driven by the global aspiration to end impunity for the gravest crimes. The Court's mission is twofold: to hold those responsible for heinous acts accountable and to prevent such crimes from recurring in the future [7].

However, the ICC is not intended to replace national courts. Instead, it acts as a court of last resort, complementing national judicial systems. This means that the ICC only intervenes when national courts are unwilling or unable to prosecute criminals.

**ICC's Judicial Proceedings:** The judicial proceedings of the ICC are designed to ensure that justice is served while upholding the highest standards of fairness, impartiality and respect for human rights.

The process works through several iterating phases, where each one could trigger the next one, or end there, if no justification to proceed exists.

Throughout the entire process, the rights of the accused are upheld, ensuring that they receive a fair trial. This includes the right to legal representation, the right to be present during the trial, and the right to be presumed innocent until proven guilty.

The different stages of the process are:

1. *Preliminary examination:* Before a formal investigation begins, the Office of the Prosecutor conducts a preliminary examination to determine whether there is a reasonable basis to proceed. This involves assessing the seriousness of the information received, the jurisdiction of the ICC, and whether the national justice system is acting on the same matter.
2. *Initiation of an investigation:* If the preliminary examination suggests that the ICC should proceed, the prosecutor can initiate an investigation. This can be done in three ways: *Proprio Motu*, referral by a State Party, or referral by the United Nations Security Council.
3. *Issuance of arrest warrants or summonses:* Based on the evidence collected during the investigation, the prosecutor can request the pre-trial chamber to issue arrest warrants or summonses for the accused individuals.
4. *Pre-Trial phase:* Once the accused is in custody, the pre-trial chamber holds a hearing to confirm the charges. If the charges are confirmed, the case proceeds to trial.
5. *Trial phase:* The trial chamber conducts the trial, where both the prosecution and the defense present their evidence. Victims can also participate in the proceedings and present their views and concerns.
6. *Judgment:* After considering all the evidence, the trial chamber delivers its judgment. If the accused is found guilty, the chamber determines the appropriate sentence. The ICC can impose prison sentences but does not have the death penalty.
7. *Appeals:* Both the prosecution and the defense can appeal the judgment or sentence. The appeals chamber reviews the decisions of the trial chamber and can confirm, reverse, or amend them.
8. *Reparations to victims:* If the accused is found guilty, the Court can order reparations to the victims. This can include restitution, compensation, and rehabilitation.
9. *Enforcement of sentences:* The ICC does not have its own prison facilities. Instead, sentences are served in prisons of states that have agreed to enforce ICC sentences.

**Evidence management:** Evidence collection assumes a fundamental role in ensuring the Court proceedings are done in a fair and expeditious way.

As there is always a time gap between the occurrence of crimes, its assessment and investigation, it is very important to ensure that the evidence collected at the latter stage as support for a possible conviction or acquittal is captured as early as possible in the process to reduce the chances of tampering with the evidence and that this evidence remains authentic and valid for assessment by the Judges' Chamber.

Another important aspect in guaranteeing the validity of evidence in the trial is the assurance that the changes in custody of that evidence are documented and following proper procedure.

There are many types of evidence, many of which can be recorded and stored digitally, such as recorded witness testimonies, multimedia content, digitized documentation, forensic tests and expert reports, among other types. All other types of content that cannot be recorded and stored digitally at a minimum require a digital record of their existence and are hence classified as evidence, even if they are accessible in place other than a digital platform or physical format.

As mentioned previously, an important aspect of evidence management is the chain of custody, and the ability of the legal team to convince the Court that the evidence remains authentic and was not tampered with. This is particularly critical for digital evidence, as much of it can have been created

when there were no witnesses to corroborate what the evidence is transmitting, possibly making it inadmissible [8].

**Blockchain Technology:** The concept of Distributed Database Management Systems has existed for many decades [9] and can be considered as the precursor of Distributed Ledger Technology, commonly known as blockchain technology and conceived in the now famous Bitcoin white paper [10]. While the former considers that all different nodes are trustworthy, the latter incorporates the element of the decentralized validation of state and transactions, thus allowing for the interaction of different actors that do not necessarily trust each other but are ruled and controlled by the network itself.

There are several architectures a blockchain solution can have, from public, fully decentralized to private controlled by one or a consortium of parties. The most important characteristics for trust in a Blockchain solution, which coincide the characteristics of a successful evidence management platform [11].

Within the scope of this research, and as discussed before, trust is critical to ensure the success of a blockchain-based evidence management platform.

Blockchain has important characteristics that altogether make it an innovative solution that could fit several-use cases. Out of the four mentioned by Meunier, the immutable source of truth use case is the one that applies to this report, as "Blockchain allows information to be time-stamped, authenticated, and immutably stored" [12].

## *1.4 Methodology*

The relevance and impact of Information Systems (IS) research may be diminished in areas where it is most needed if it does not include a robust element of applied research solutions [13].

Two main paradigms dominate the field of IS study. One of these paradigms revolves around behavioral science, which seeks to formulate theories predicting individual and organizational behavior. The second paradigm, design-science, focuses on enhancing the capabilities of individuals and organizations by creating innovative artifacts [14].

In this context, this research utilizes the Design Science Research Methodology (DSRM) and the six principles put forth by Peffers and his colleagues [13]. With a foundation in engineering and the artificial sciences, this approach aims to develop useful artifacts that contribute positively to their respective domains of application. As per the authors, the DSRM process consists of a typical sequence of six activities, for details see [13].

The artifact to be created in this research is the creation of a conceptual framework, denominated as MultiTrustBloc (MTB). It has a problem-centered initiation, and it followed all the steps until the communication stage.

An important part of validating the output of such a method was to assemble a panel of experts who would validate the problem and evaluate the artifacts. The panel consisted of three individuals who combined have decades of experience in ICCs. Due to the sensitive nature of their jobs, personal identifiable information from the panel members remains anonymous. The panel of experts, however, consists of members who have a combined amount of relevant experience of over 35 years, of male and female representatives, and from different continents. The area of work of each of the three was as diverse as possible within this environment, one being an IT specialist, another a legal specialist in victims and witnesses and the third one had several years' experience in the prosecution side.

An initial meeting was held in the month of June of 2023 to capture the needs and objectives that such research could bring to the delivery of justice in an international criminal justice context. The evaluation criteria and objectives of each were discussed and selected as guideposts for this work.

The evaluation stage of this methodology is also a critical one, to ensure the benefits of the created artifacts are realized. As such, having a way to measure them objectively and agnostically is very important. Prat *et al*. propose a systematic list of for evaluating artifacts, which is organized by a hierarchy of criteria within dimensions that they consider complete and mutually exclusive [15].

For the evaluation of the created framework, the previously described panel of specialists provided their expert knowledge by validating the solution presented in this research. The artifact was measured based on the following objectives: Through a survey, these specialists evaluated the framework based on the evaluation criteria set, which was then specified in Table 1. The evaluation method decided was a survey based on a 5 point system Likert scale [16], where 1 was "Strongly Disagree" and 5 was "Strongly agree".

***Table 1.*** - Defined objectives to be measured by the specialists.

| Dimension | Criteria | Objective |
|---|---|---|
| **Goal** | Validity | Meets the principles of robust evidence management and chain of custody. |
| **Environment** | Consistency with organization / utility | Provide ICC with a clear and easy to identify chain of custody of evidence. |
| **Environment** | Consistency with technology / harnessing of recent technologies | Makes use of blockchain technology capabilities to improve efficiency, effectiveness, and the fairness of judicial proceedings. |
| **Structure** | Completeness | It is a solution that could meet at least 80% of the current requirements with regards to evidence management, from collection to disclosure. |
| **Activity** | Accuracy | Meets the requirements it was intended to fulfil. |
| **Evolution** | Robustness | Can resist outages, and attacks to the integrity, availability and confidentiality of data. |

### *1.5 Overview of this research*

As this chapter describes the context, motivation and objectives of this document, the following chapters aim to present the knowledge created by the writing of this research. They are as follows:

**Chapter 2: Blue Ocean strategy analysis.** Adopts this analytical framework to confirm that a blockchain-based solution would add value to the evidence management process within international criminal justice. A qualitative comparison is made between existing evidence management solutions and a blockchain-based one, identifying each one's characteristics within the Blue Ocean framework.

**Chapter 3: Literature review.** It makes use of the PRISMA [17] methodology to perform a systematic literature review on the topics covered in this research, including a comparative analysis of five dimensions, namely blockchain, chain of custody, evidence management, multi-level trust and the public sector.

**Chapter 4: MultiTrustBloc framework design.** It describes the blockchain-based solution for evidence collection, management and disclosure. It provides an extensive detail of the solution, from multiple perspectives and finishes with the evaluation of the panel of experts on the artifact proposed.

**Chapter 5: Conclusions.** This final chapter wraps up the findings and includes the final activity of the DSRM module, which is the communication that was performed regarding the knowledge that was produced, including the approval for publication of two conference papers based on this research.

## 2 Blue Ocean Strategy analysis

### *2.1 Identification of current body of knowledge*

The Blue Ocean Strategy [18] was invented in 2004 and it analyzes innovations that enable the creation of uncontested market spaces that make the competition irrelevant. This strategy, in its essence, helps create a roadmap that enables businesses to create or venture into new markets and become able to keep costs down and reduce competition [19].

A search for Blue Ocean Strategy applied to the judicial system was done in three databases (Scopus, ACM Digital Library and IEEE) on 11/10/2023, with the following string:

"Blue Ocean Strategy" AND (Court OR Judicial OR evidence)

Only a total of 22 articles were found in the combined databases, and having looked at the title of each one of them, none made reference, direct or indirect, to the judicial sector, as the results only arose from a combination of the first term with the work evidence. Alternatively, using the following string returned only one result [20]:

"Blue Ocean Strategy" AND Blockchain

The search string with only "Blue Ocean Strategy" returned almost 300 results, and after a high level analysis on the titles of the documents, it was clear that this strategy has been researched in a broad range of areas, such as the banking industry [20], academia [21], small and medium enterprises [19], logistics [22] and many others.

Transposing this strategy to the area of international criminal justice, as each court has a welldefined mandate that is mutually exclusive, the origination of this type of strategy focuses on their evidence management capabilities from a general perspective.

## *2.2 Strategy Canvas approach*

The authors have several years of combined experience in blockchain, public sector, and national and international judicial systems within technology areas. The identification of major characteristics of current judicial evidence management systems was done alongside identifying what characteristics they could incorporate to improve and leapfrog the current state.

Using the Four Actions Framework [18], a comparison was done between traditional evidence management systems and a blockchain-based one, hereinafter denominated MultitrustBloc, or MTB.

**Factors considered** - *Eliminate* - Reliance on controlling party for evidence integrity: It reflects that evidence is at the mercy of the party who controls it. Only when the evidence is disclosed will other parties be able to guarantee the immutability of the evidence and have different copies of the same evidence.

MTB resolves this by keeping an immutable record once the evidence is registered through the creation of a digital signature that is stored in the solution and decentralized and replicated among other nodes.

Witness corroboration required: Due to the usual long lead time between evidence collection and disclosure and presentation in the Court, it is often required for at least a witness to validate the veracity of evidence being presented. Additionally, the relative ease of tampering with the data requires a third party, for example a witness, to validate the evidence's authenticity.

MTB: By creating a digital signature before the evidence is considered as such, and by replicating it, the Court and its judges will have many more guarantees of the authenticity of the evidence, without resorting to other ways of corroboration.

*Reduce* - Evidence tampering vectors: There are several points of time that the evidence can be tampered with, or accessed without permission, depending on the security level of the custodian, from collection, to custody, to handing over, there is a low visibility and higher chance than desired that evidence could be adulterated.

MTB: By creating a signature of the evidence early in the process, any change to it will be detected as not complying with the original registration of the data, meaning that from that point on, the record is immutable.

Multiple copies of the same evidence: For digital evidence, it is very likely that depending on the mean of storage, the evidence is copied multiple times, leading to increased chances of leakage and tampering.

MTB: Allows for having a clear identification of where the evidence is, and if in digital form, to have it directly linked with the evidence record, allowing that the parties with access to access the same file directly without having each one use a different place to access it.

*Raise* - Streamlined chain of custody: Ensuring that the evidence was always within the possession and control of a trusted custodian is of paramount importance to help guarantee the authenticity and integrity of the evidence.

MTB: Every single change in the evidence is recorded, ensuring that any change in status is well accounted for and should there be any need, all changes can be easily identified and retrieved.

Scalable evidence reviews and sharing when a legal team receives a piece of evidence from a third party, requires it to be registered and for them to perform their due diligence to minimize any possibility that the evidence appears inauthentic or invalid in Court. Each piece or batch of evidence received requires processing from the very beginning.

MTB: Keeps the log of all changes in the data and allows for accredited organizations to first review the data, and then share it with the legal team for their review. This will allow the latter to have much more information about the evidence, including its origin and if any analysis has been done on it.

Cooperation with interested entities: The IJC relies on a wide range of entities to source evidence that could support the building of a case, as many times it has no physical direct access to persons or areas of interest.

MTB: Opens the network to trusted and non-trusted partners as it allows the former to register possible evidence in the solution, and thus do much of the preparatory work that needs to be done. It also empowers these organizations to become more active as they are able to have a bigger impact on fulfilling their objectives. *Create* - Digital evidence and associated record shared synchronously:

The evidence and the chain of custody are two different artifacts that attempt to be in as much synchrony as possible, however it is very possible that both are kept in different areas and that linkage could easily break due to human error or an outsider's action.

MTB: By creating a strong link between the evidence record, including the chain of custody and the evidence itself, the solution can provide cohesive management of both the evidence and the record.

Realtime chain of custody: As it is built nowadays, the chain of custody is normally done in manual form and each team or entity could have their own protocols.

MTB: Establishes a standard regarding the chain of custody. It is also extremely easy and quick to retrieve the whole chain of custody of evidence, by retrieving all the blocks created by the change of status during its lifetime.

## *2.3 Strategy Canvas*

To represent this in a visual form, a Strategy Canvas [18] has been designed to take into consideration the factors mentioned above. **Figure 1** depicts how MTB fits into the incumbent evidence management solution.

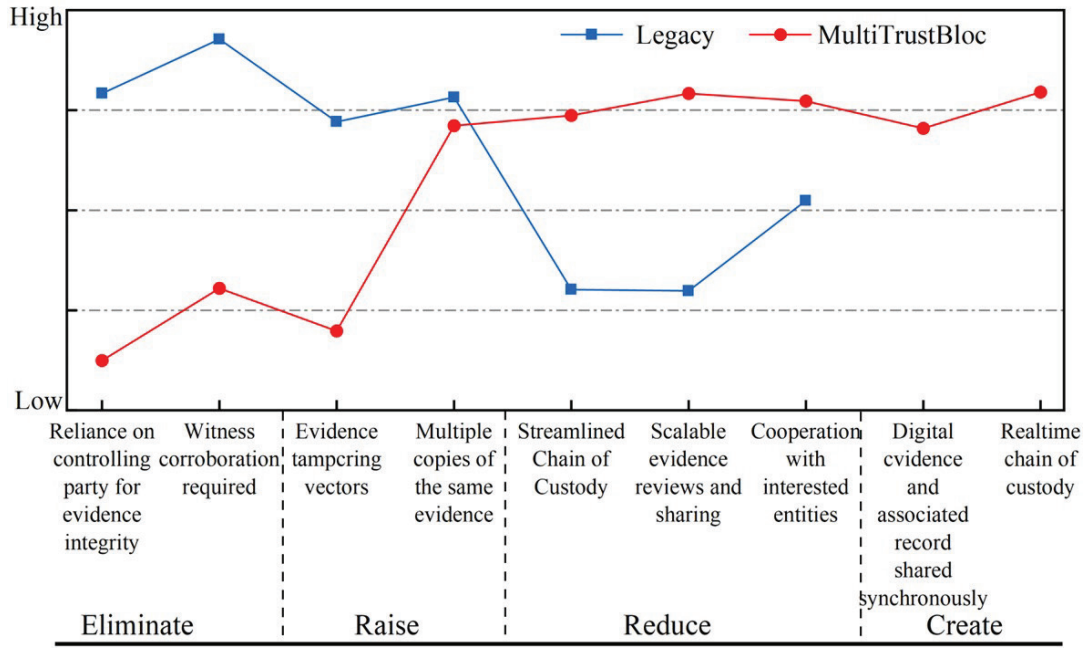


***Figure 1.*** Strategy Canvas for current Evidence Management solutions and MTB

**Validating the Blue Ocean Characteristics**

The authors that coined the Blue Ocean strategy [18] established a five-point checklist for understanding if an innovation fits its strategy. This sub-chapter compares the MTB with those same requirements:

*Creates uncontested market space?*

Yes. While ICCs don't have competition, by implementing such an innovative solution, their reach will expand by allowing other entities to participate in their activities. It creates a platform where (potential) evidence could be registered, even before the legal team has the approval to investigate a specific situation.

*Makes the competition irrelevant?*

Not applicable, each court has a unique and very well-defined mandate.

*Creates and captures new demand?*

Yes. It allows a multitude of organizations to directly participate in its activities and help pursue the accomplishment of its mandate.

*Breaks the value-cost trade-off?*

Yes. It becomes a matter of trust and confidence that the data are correct. Teams and judges can focus on the content rather than on its authenticity.

*Aligns the Court's activities in pursuit of differentiation and low cost?*

Yes. Tasks such as chain of custody verification or evidence integrity are drastically reduced, since it is done automatically, and easily confirmed. Time and effort are dramatically reduced, also because digital evidence will require less corroboration, meaning less witnesses in the courtroom testifying, thus, less costs in this activity. These can be particularly high.

## 3 Literature review

After concluding that a blockchain solution could add value to international criminal justice, when compared with the current systems, a systematic literature review was made using PRISMA methodology [17]. The selection of the studies to be included in this review, and within the scope of this research, consisted in all studies that focused on blockchain and the use case of the chain of custody within the legal or investigative areas. The search string chosen, was therefore, the following:

Blockchain AND "Chain of Custody" AND (Court OR Judicial OR Evidence)

The sources of this identification were four databases (Scopus, Web of Science, ACM Digital Library and IEEE) with which ISCTE has access agreements and were accessed on the 22nd of June 2023.

A total of 65 documents were screened, after removing a total of 41 duplicate records from the databases searched. A total of 12 were not able to be retrieved without incurring additional costs. There were 8 studies with IoT in the title that were removed as this deviates from the purpose of this research.

Once the first screening of studies was concluded, 45 articles were assessed for eligibility. There were 15 of these that had an abstract which was not relevant, and for 3 of them, after analyzing the whole article, 2 didn't fit the scope of the research and 1 was in essence a duplication of another relevant article, despite the different title.

In summary, 27 studies qualified for the systematic review, as depicted in Figure 2.

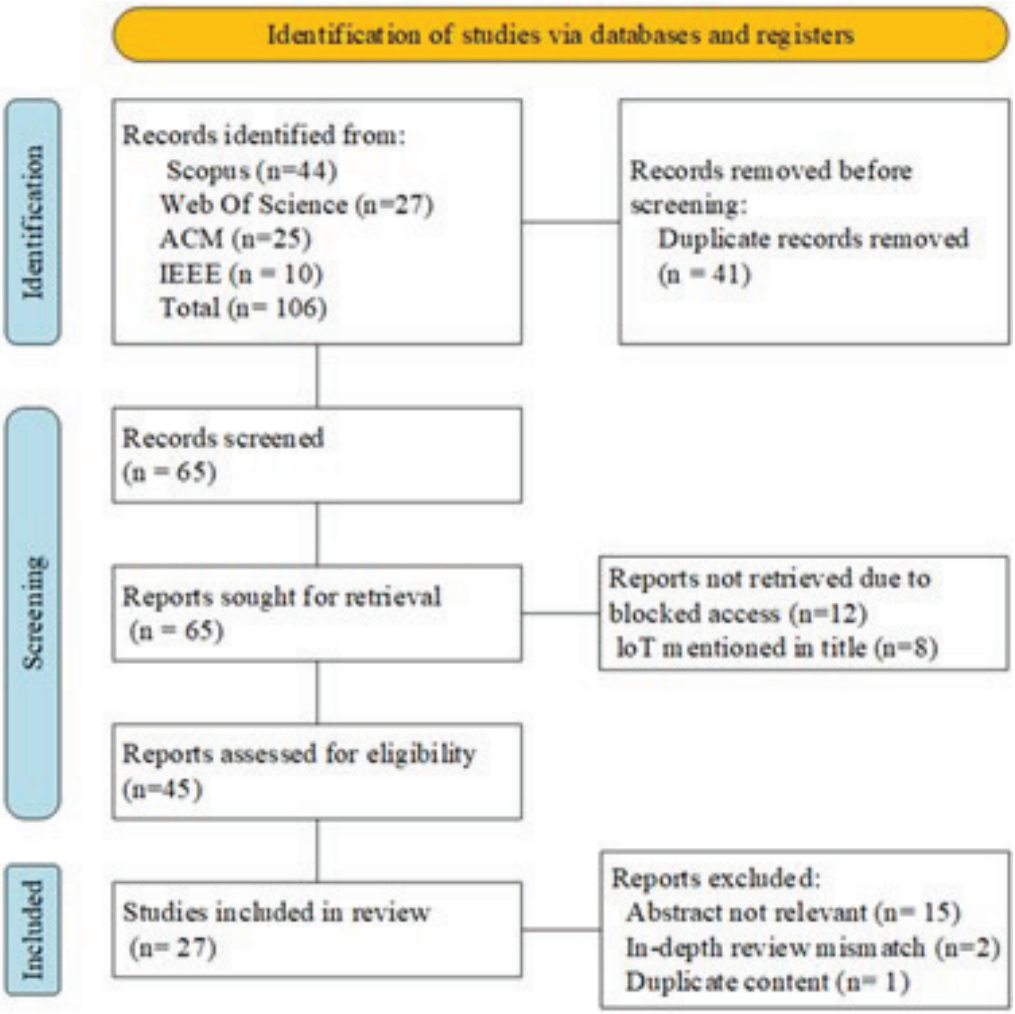


***Figure 2.*** - PRIMA instance of the literature review for this research

### *3.1 Studies reviewed*

The literature around this topic is still very nascent, with the first related study being published in 2018. Figure 3 shows an increased interest in this topic, despite the trough that occurred in 2022, with only 3 studies published.

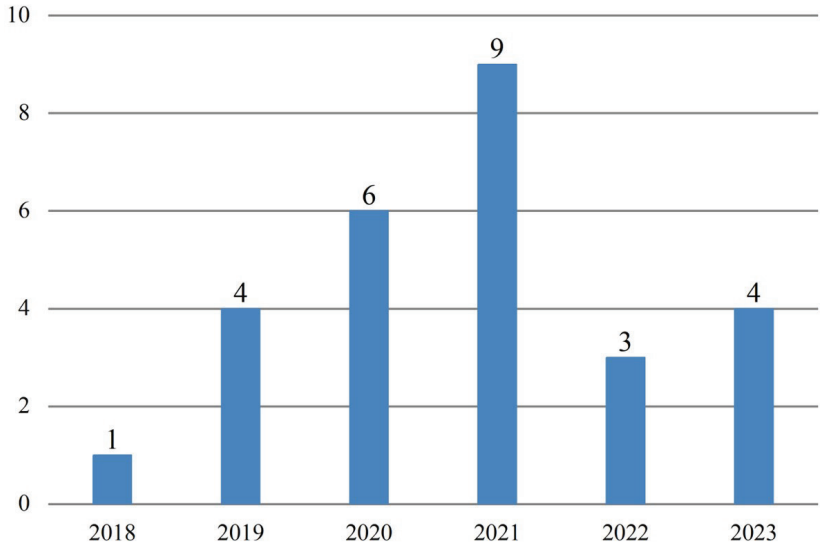


***Figure 3.*** - Number of eligible articles published per year

In this chapter, a variety of articles related to the intersection of blockchain technology and the chain of custody are discussed and evaluated, focusing primarily on the applicability of blockchain to improve the integrity, authenticity, and secure handling of digital evidence within a legal and public sector context.

The studies were assessed on 5 key attributes that compare with the area of this research, being:

1. Blockchain: Does the solution rely on blockchain technology?
2. Chain of Custody: Is there a mechanism to guarantee a chain of custody for data in particular evidence?
3. Evidence Management: Does the solution offer evidence management capabilities, through the evidence lifecycle?
4. Multi-Level Trust: Does the solution support the transfer and/or access of data by different, independent, parties?
5. Public Sector: Is there a use-case identified for organizations in the public sector?

Based on these categories, the articles were reviewed and grouped based on the same matching categories to more clearly understand the area they focus on and how it relates to this research.

**Group A – Research on solely blockchain and chain of custody attributes** - This group is represented by 4 studies focused solely on the blockchain and chain of custody attributes. Given the complex interplay between social systems and technology, the authors of [23] discuss blockchain through a sociotechnical lens. This perspective offers a more nuanced understanding of the technology, including its societal implications and potential applications. They highlight that blockchain technology could revolutionize the chain of custody process due to its inherent characteristics like transparency, security and immutability. As with any new nascent technology, they argue that it is very hard to predict the path blockchain will take and propose a learningbydoing approach to better understand blockchain's capabilities and limitations.

The article by Olukoya [24] provides an analysis on how blockchain technology can be integrated with incident response software to enhance digital investigations. The author suggests that a blockchain ledger can serve as a powerful tool for preserving the integrity of security investigations and associated metadata. Building on models from an open-source incident management platform, he proposes a framework using blockchain technology to ensure the authenticity and immutability of forensic findings and subsequent analysis actions. The stored data on the blockchain, being immutable and verifiable, provide a robust audit trail for every action taken during an investigation.

The topic of multimedia digital forensic investigations and securing the exchange of multimedia data over the internet is discussed in [25]. The authors emphasize the pressing need for solutions that can ensure the integrity, reliability and trustworthiness of multimedia investigations and introduce

a solution based on Blockchain Hyperledger Sawtooth to which they call MF-Ledger. The solution permits these stakeholders to form a private network where they can exchange information and reach consensus on different investigation actions. The authors argue that this addresses some of the key challenges facing the multimedia industry in the era of global digital connectivity and heightened cybersecurity risks.

The article in [26] discusses the proposal of a tamperproof timestamped provenance ledger (TTPL) utilizing a public and trusted blockchain. It offers various levels of integrity verification, and has been designed with a focus on privacy, with scalable characteristics. The authors highlight the feature that allows the data originator to create a permanent proof via a web browser, demonstrating they had access to potentially sensitive data at a specific point in time. This proof can be generated without compromising, revealing, or externally storing any sensitive information. Additionally, this proof is anchored in a timestamped provenance record contained within a public blockchain.

**Group B – Research addresses evidence management with chain of custody on blockchain, but not on multi-level trust nor the public sector** - This group includes 7 studies that not only address blockchain and chain of custody attributes, but also incorporate evidence management.

The article [27] addresses the current challenges in evidence preservation technologies, which heavily rely on standalone cryptography technology, making them susceptible to tampering. Liu *et al*. propose a data preservation model that is based on a decentralized blockchain bolstered by smart contracts. The integration of smart contracts automates the management and verification of this process, significantly reducing the likelihood of human error or tampering and the utilization of blockchain technology in this context provides a decentralized, immutable ledger to record the handling of evidence, thus enhancing its security and integrity.

The authors in [28] underline the vital role of the chain of custody in demonstrating that digital evidence has not been tampered with during any phase of an investigation. Their work is focused on digital image forensics, combining the use of grey hash and blockchain technologies. Grey hash is a form of digital fingerprint for images, and combined with blockchain they present a robust solution for maintaining the integrity of the digital evidence.

Sathyaprakasan and co-authors delve into the fundamental concepts of block-chain and the chain of custody [29]. They bring forward a high-level framework for managing digital forensic evidence utilizing Hyperledger Fabric, a permissioned blockchain infrastructure. They focus on illustrating how blockchain technology can be effectively applied in the domain of digital forensics. The framework they propose aims to integrate the chain of custody (the process of documenting the movements and locations of the evidence from the time of collection) into the Hyperledger Fabric.

Another proposed solution that tackles the problem of evidence management within a resilient chain of custody supported by blockchain is presented in [30]. The authors propose a solution that integrates private and public blockchains, where the public blockchain acts as a guarantor of data integrity and decentralization. By doing so, they aim to create a system that is not only reliable and secure but also allows for independent verification of the evidence's chronological journey.

Another work within this group is [31], where the author devises a blockchain-based solution named CustodyBlock to support the chain of custody and integrity of digital evidence. It also aims to facilitate transparency and trust between different parties involved in the evidence's life cycle, from its initial collection to its use in legal proceedings.

In [32], the authors propose a system that fuses blockchain technology with machine learning in the form of K-means clustering. The K-means clustering technique is used to determine the storage location of the digital evidence. The primary focus of the proposed system is the security of digital evidence information. The use of machine learning techniques aids in efficient and secure data storage, making the retrieval process more manageable and efficient.

Another blockchain-based solution for managing digital evidence was identified in [33] with the characteristic of also tracking the entities accessing this data as a major differentiator from other proposals. This feature is crucial in maintaining a secure chain of custody for digital evidence and ensuring that the evidence has not been tampered with during the investigation process. Additionally, the Proof of Work (PoW) consensus algorithm is employed to verify the integrity of the blocks in the blockchain.

**Group C – Research covering all attributes except 5., the Public Sector** - This group of 8 studies extends to cover all attributes except the public sector area. Zhang *et al*. [34] focus their research on cloud forensics and identify an approach to validate the provenance of digital forensics from cloud service providers from different jurisdictional areas. It bases the system in a certificate authority that guarantees the anonymity of the users.

Looking at the topic from the viewpoint of mobile forensics, the authors in [35] identify that while current mobile forensic tools are primarily concerned with the efficiency of data extraction, it is very important to maintain the integrity of such data for their use as evidence in the Court. They propose a specially designed blockchain system built from the ground up to fulfil the requirements of preserving digital evidence.

The authors in [36] explore the potential of utilizing blockchain technology in the management of the chain of custody. They propose the use of a private and permissioned blockchain, showing its applicability in this context. They also evaluate the performance of this system, illustrating the practicality and effectiveness of their solution for the management of digital forensics evidence. They address the essential requirements of a chain of custody (CoC) process which include integrity, traceability, authentication, verifiability and security (being tamper-proof).

In [37], the authors utilize blockchain technology and specifically incorporate a Boneh-Lynn-Shacham signature, known for its short signature size and efficiency. The unique aspect of their proposal is the integration of attribute-based encryption for fine-grained access control. This means that access to the evidence is controlled based on the attributes of the user or the evidence itself, ensuring that only authorized individuals can access specific pieces of evidence. This approach offers an added layer of security and control in the management of digital evidence.

The article [38] introduces a blockchain-based framework for managing digital evidence in a manner that a multitude of stakeholders can accept it. The proposed framework aims to ensure the integrity and immutability of digital evidence. Through this approach, the authors aim to create a real-time, tamper-proof method of managing digital forensic evidence that can effectively meet the demands and challenges of modern forensic investigations. It is constructed in three logical layers:

- The evidence layer: This layer supports a trusted storage medium for digital evidence, ensuring its safety and authenticity.
- The blockchain-based layer: This layer is where the blockchain technology operates, providing a decentralized and secure system that guards against tampering and allows for the verifiability of the stored evidence.
- The network layer: This layer provides peer-to-peer connectivity among all parties that come into contact with the evidence. It facilitates communication and cooperation between different stakeholders.

The article [39] presents a blockchain-based system designed to maintain digital forensics' chain of custody. In this system, the authors introduce a method for managing and exchanging data between different parties, ensuring the integrity and verifiability of the digital evidence. The solution they propose includes several key capabilities such as:

- Evidence Creation: The ability to record and store digital evidence securely.
- Evidence Hash Transfer: The use of cryptographic hash functions to maintain the integrity of digital evidence while it is transferred between different parties.
- Evidence Display: A mechanism for transparently displaying the digital evidence to all relevant stakeholders.

Through these features, the system created by Chopade *et al*. ensures that the chain of custody in digital forensics is maintained, thus enhancing the credibility and trustworthiness of the digital evidence.

The authors in [40] explore how blockchain technology can be utilized to ensure the authenticity and legality of various processes and procedures in the realm of digital forensics. They recognize the need for a comprehensive view of transactions that affect specific data, extending back to their origin and propose using blockchain technology to create an immutable record of these transactions. To validate their concept, Lone and Mir present a proof of concept using Hyperledger Composer and finalize the study by measuring the performance of their proposed architecture, demonstrating the potential effectiveness of their blockchain-based approach to managing the chain of custody in digital forensics.

The last article within this group focuses on a practical case study for the creation of smart contracts for managing the chain of custody of digital evidence [41]. It expands on previous work conducted by Bonomi *et al*. [36]. The authors focus on exploring different aspects of the chain of custody in digital forensics, specifically examining different architectures: Centralized, distributed, and multi-blockchain. The authors focus particularly on distributed architecture, which can provide decentralized

and tamperresistant record-keeping, enhancing the integrity and traceability of digital evidence. To showcase the practical implementation of their ideas, the authors develop a prototype system using a distributed architecture combined with smart contracts. These smart contracts incorporate a zero-knowledge proof, a cryptographic method by which one party can prove to another that they know a value, without conveying any information apart from knowing the value.

**Group D – Research covering all attributes except 4., multi-level trust** - This group of 5 studies covers every attribute except for multi-level trust, emphasizing public sector applicability. With a focus on log files gathered from a Cloud Service Provider (CSP) [42], the authors identify and analyze the benefits of incorporating blockchain into the process of capturing and maintaining log files in a cloud environment. They also compare this approach to the conventional methods of collecting and preserving forensic evidence.

In the article [43], the authors devise a blockchain-based chain of custody solution that introduces the concept of a "digital witness". These digital witnesses are named "Hearsay Digital Witnesses" as they are designed to identify, retrieve and securely store digital data, functioning as a layer of data replication that further secures the evidence.

Another study fitting within this group is called LEChain [44]. It is designed to oversee the entire judicial process, from evidence collection during police investigations to jury voting during court trials, utilizing blockchain technology to supervise the entire flow of evidence as well as all courtrelated data.

In [45], a blockchain-based evidence management system is discussed as a way to address the challenges of evidence tampering and obstruction of justice prevalent specifically in South Asia. They propose a solution in the form of a hybrid blockchain-based system designed to create a tamper-proof environment for storing and handling evidence. The system is designed to protect the identities of whistleblowers and offers the option for the original uploaders of confidential evidence to disclose it if they believe the involved parties are not acting appropriately.

In [46], Tsai presents an approach to managing evidence within criminal investigations by leveraging the capabilities of blockchain technology, namely the Ethereum [42] platform, supplemented by smart contracts.

**Grouping E – Individual studies which had unique coverage of attributes** - This group of 3, represents individual studies each with unique coverage of attributes. Sanda *et al*. [47] focus their contribution within the cloud service providers sector, specifically in virtual machines running within those cloud providers. They address the challenges and solutions related to maintaining evidence integrity in cloud forensics. Acknowledging the potential for collusion among stakeholders to tamper with evidence, it emphasizes the crucial role of blockchain in ensuring the integrity of cloud forensic artifacts, such as cloud logs, chain of custody and file metadata. The authors don't identify how the evidence management process could be supported.

Akello *et al*. [48] explore the potential of blockchain technology in addressing gun violence issues, especially in the United States. They propose a blockchain-based framework that enables tracking the chain of custody of firearms as they are transferred between individuals. This study doesn't cover multi-level trust nor evidence management.

The authors of [49] propose a data preservation system called BoCA (Blockchain-of-Custody Application), which is compatible with various blockchains, including Ethereum and BitCash. Their solution allows one to store data, encrypted or otherwise, in a transparent and verifiable manner.

## *3.2 Literature review conclusions and gaps identified*

The literature available within this topic clearly demonstrate the increased attention to the value of blockchain to maintain the tamperproof chain of custody and to support the management of evidence on those platforms. Several types of blockchain can be used to implement this and the configuration can be done differently focusing on specific needs from the researchers. It is clear how blockchain technology can improve the resiliency and integrity of a chain of custody for many areas, including forensic analysis or evidence management. The studies analyzed approached this subject in different and novel ways. During the systematic review no study would encompass all five attributes this research aims to focus on, and as such, this is an important addition to the body of knowledge within this area. ***Table 2*** depicts the studies, grouped by attribute set.

Other gap that was identified in the literature reviewed is the absence of use cases and solutions tailored for the international legal public sector, or a sector where a network of providers feed the main entity with evidence.

***Table 2.*** - Literature review overview and comparison with this research

| Group | Blockchain Framework | Chain of Custody | Evidence Management | Multi-Level-Trust | Public Sector |
|---|---|---|---|---|---|
| **A – Research solely on blockchain and chain of custody attributes** | Y | Y | N | N | N |
| **B – Research addresses evidence management with chain of custody on blockchain, but not multilevel trust nor the public sector** | Y | Y | Y | N | N |
| **C – Research covering all attributes except 5., the public sector** | Y | Y | Y | Y | N |
| **D – Research covering all attributes except 4., multi-level trust** | Y | Y | Y | N | Y |
| **E - [47]** | Y | Y | N | Y | Y |
| **E - [48]** | Y | Y | N | N | Y |
| **E - [49]** | Y | N | Y | N | N |

## 4 MultiTrustBloc (MTB) Framework

In the realm of international jurisprudence, the ICC stands as a beacon for prosecuting heinous crimes that resonate on a global scale. A pivotal component of this mandate is the meticulous management and authentication of evidentiary materials, which are frequently procured from a myriad of sources, encompassing national judiciaries, non-governmental organizations, and other international entities. These conventional systems, while comprehensive, occasionally grapple with challenges related to ensuring unbroken chains of custody and the inviolability of evidence. The potential for human oversight, inadvertent errors, or deliberate manipulation cannot be entirely discounted. Given this backdrop, a compelling exigency emerges for an innovative, impregnable, and streamlined system dedicated to evidence management and authentication.

The ICC could grapple with challenges pertaining to evidence management, particularly in ensuring the authenticity and chain of custody of evidentiary materials. This chapter elucidates the objectives of integrating a blockchain solution, hereinafter called MTB within the ICC's operational framework, specifically addressing the identified problems:

- **Ensuring Tamper-Proof Evidence Management:** To establish an immutable and chronological record of evidence, ensuring that it cannot be altered retroactively once an item is entered into the blockchain.
- **Facilitating Transparent Chain of Custody:** To create a transparent and traceable record of every interaction with a piece of evidence, from its inception to its eventual use in court proceedings.
- **Streamlining Collaboration with Third Parties:** To foster a seamless and secure platform for collaboration between the ICC and external entities, ensuring that evidence shared by third parties retains its authenticity and integrity.
- **Enhancing Verification and Authentication Processes:** To expedite the process of evidence verification, ensuring rapid yet robust authentication mechanisms.
- **Bolstering Public Confidence and Accountability:** To enhance the public's trust in the ICC's evidence management processes, ensuring that justice is not only done but is seen to be done.

As the MTB solution aims to support the whole of the Judicial Lifecycle of the ICC, therefore distinct actors are involved at different stages of the process. ***Table 3*** describes the roles each one of them have, together with a description of the privileges they would have at different stages of the process.

***Table 3.*** - MultiTrusBloc identified roles

| Role | Description | High level view of permissions |
|---|---|---|
| **Prosecution team** | Determines the data deemed as evidence and submitted to the Court chamber. | Until evidence disclosure, the team can view and control any artifact within the MTC. |
| **Accredited entity** | The entity cooperates with the prosecution team to identify and gather information, either directly or through trusted partners. | it can create and submit evidence records in the MTC, accessing the artifact until the prosecution team takes ownership. |
| **Non-accredited entity** | May include civil organizations or citizens seeking to expose committed crimes. | Submits potential evidence to an accredited entity or the prosecution team for evaluation. |
| **Court chamber** | Assesses submitted evidence and delivers judgement accordingly. | Receives and takes control of the evidence once handed over by the prosecution team. |
| **Involved third parties** | Have different objectives and could represent different people or groups in the specific case | Parties such as the defense or victims' representatives may require evidence disclosure to participate in the proceedings. |

## 5 Process Flows identified

This process starts in the moment that any entity identifies an artifact as potential evidence, and depending on the actor, it is automatically added to the MTB or submitted for review. A visual depiction of the process can be found in Figure 4, using BPMN [34].

The process can have multiple starting points, and what differentiates them is the stage in the process they start in, and what actor triggers it.

1. *Submits data to accredited entity:* The entity, holding potential valuable information contacts an accredited organization that has a direct relationship with the Court.
2. *Validates suitability of data:* When the data are received, the receiver will validate its suitability against the ICC's Rome Statute [2] and rules of procedure and evidence [3].
3. *Informs local citizen/entity of its inadmissibility:* If the data provided doesn't meet the minimum admissibility threshold, the evaluator informs the entity that submitted the data that it cannot be considered as evidence and will not be processed further.
4. *Treats data as evidence and creates snapshot:* If the analysis results are positive to potential evidence admissible to the ICC, the accredited entity will ensure the record is ready to be submitted to the MTB for the prosecution's assessment. The evidence is stored and baselined to ensure no future tampering possibilities. This could be the first activity of the process, if the accredited entity is the one acquiring the evidence.
5. *Creates records in MTB:* As soon as the data are ready for submission, the accredited entity will create a record in the MTB, meaning the first block for this artifact is created. A notification will be sent later to the prosecution team for review.
6. *Reviews Evidence:* As the prosecution team is notified, it will review the submission by the accredited entity, based on the current status of the existing or potential case. During the review process, the MTB is accessed and any changes to the record will be reflected through the creation of new blocks. The outcomes of this review will decide on the suitability for the case.
   a. Updates record in MTB setting status as inadmissible: If the review outcomes are unsatisfactory, a new block in the MTB is created to reflect this update.
   b. Informs accredited entity of its inadmissibility: The prosecution team informs the accredited entity with the conclusions of its review.
7. *Creates record in MTB:* Derives from the prosecution team's direct action, which has acquired evidence at the source and creates the record immediately.
8. *Updates record in MTB and retrieves evidence to its control:* The record in the MTB is enriched with additional relevant metadata that is required to fulfil the acceptable criteria for judicial evidence. The status of the artifact is updated and committed with the creation of a new block

in MTB, and the record is finally accepted as evidence. Once the submission is analyzed and considered as evidence, it resides under the prosecution team's custody for review and for building a case against a suspect. This process starts with the need to evaluate specific evidence, visually depicted in Figure 5.

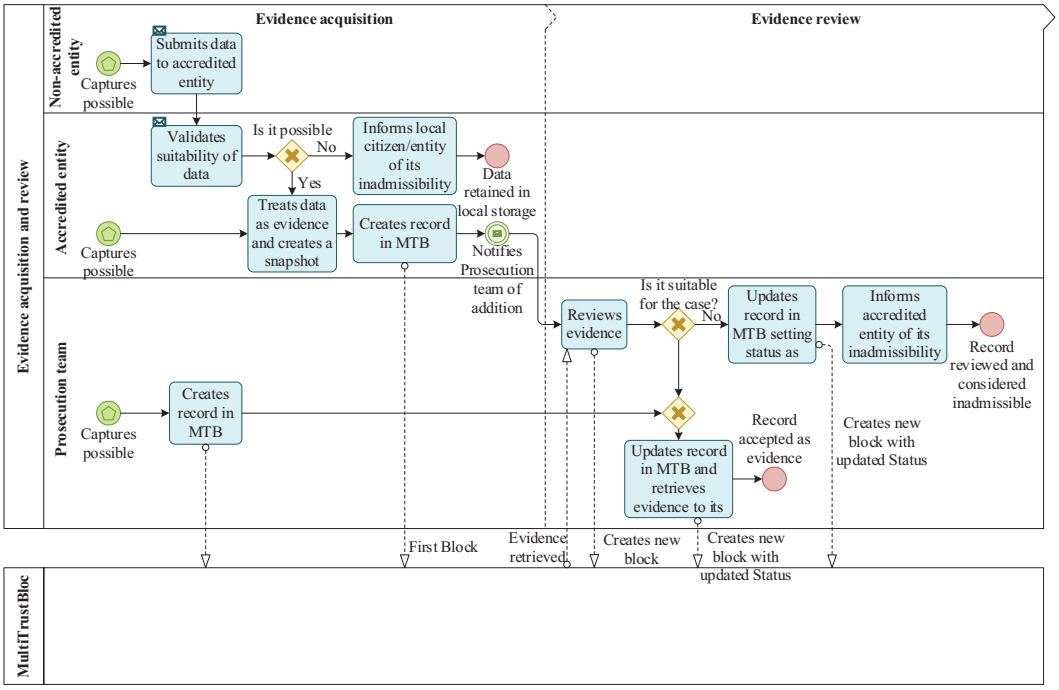


***Figure 4.*** - Evidence acquisition process

9. *Reviews evidence:* The prosecution team fetches the evidence record from the MTB and does the analysis it needs within the context of its mandate.
   a. Reads the data: In case the review doesn't require an update to the record, the action is only to read the data within the record.
   b. Updates the record: If there is the need to update the record with the outcomes of the review, the changes are written and committed into the MTB by creating a new block to represent such actions.
10. *Closes record:* Once the actions are done and the judicial process remains in the same stage, the record is closed and the process finishes then.
11. *Prepares disclosure:* If the evidence becomes relevant to advance to another state and be shared with other parties, the prosecution team will prepare its disclosure.
12. *Selects privileged participants:* As the disclosure process requires the sharing of evidence to third parties, the prosecution team identifies which participants will assume specific privileges. For example, which (pre-)trial chamber will assume ownership of the record and evidence and which other teams can access it, such as the defense or victims representatives' teams.
13. *Submits record disclosure:* The prosecution team commits the updates and a new block is created to reflect the ownership and access rights changes.
   a. Hands over ownership of record and data: After submitting the record disclosure, the prosecution team transfers the evidence to the chambers' data repository and relinquishes its ownership.
   b. Receives ownership of record and data: the judge's chamber is notified of evidence transfer and custody is in their control.
   c. Receives notification of access to the record: Involved parties are notified that new evidence is available for their review.
14. *Accesses the record:* All three actors, throughout the different judicial stages, access the record as required and if they have the rights, they will add new blocks to reflect changes in the record. This could be actions like presentation in court, link to another case, etc.

Once the different judicial stages are concluded, the process ends.

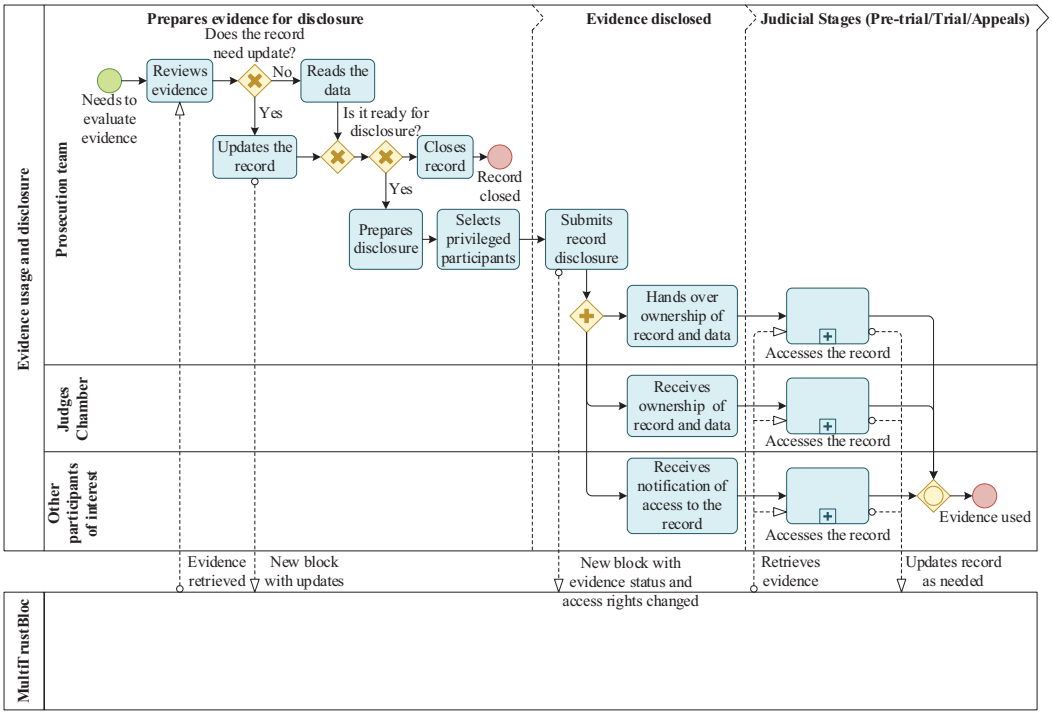


***Figure 5.*** – Evidence usage and disclosure process

## 6 High level system overview

As designed, the MTB is a registry for the status of an artifact with potential evidentiary value for a crime within the ICC's jurisdiction which is decentralized and thus, tamper-proof. As such, it allows holders of potential evidence to submit their evidence to an entity accredited by the ICC, meaning that it is allowed to add a record in the MTB to register it as potential evidence before evaluation. The ICC's prosecution teams could have the role of accredited organization, for allowing direct contact with sources.

When the accredited entity receives the submission and deems it suitable to share with the prosecution team, a new record is created with the possible evidence baselined.

The accredited entity further validates the submission, and it is moved to the respective repository, which the prosecution team has access to.

Should the prosecution team identify the artefact as valid evidence for their case, they will reflect that in the MTB and proceed to transfer the evidence into their custody. As the evidence is used, the MTB will be creating new blocks in the chain to reflect the change in status of that same evidence. Participants in the case will have different types of access to the records, depending on the state of that evidence. At the solution's foundation, there is a consortium between the prosecution, judiciary and other interested parties to make it robust, credible and tamper-proof. Figure 6 provides a high-level view of how the system will interact with evidence and multiple parties.

**Roles and Responsibilities -** The MTB is supported by two groups of entities that bring different roles to the solution. The first and critical group is represented by the Court's chambers and the prosecution (teams). These are the main decision makers on the future of the solution and permanent members of it. They propose and validate transactions, manage and change smart contracts, and have a final say in any disputes or changes to the blockchain's protocol. The other is the secondary entities group, consisting of any accredited entity by the primary entities that wishes to participate in the advancement of justice, helping to maintain the blockchain and validate new blocks.

**Consensus Mechanism -** Given the consortium characteristics of this blockchain, the consensus mechanism selected was Practical Byzantine Fault Tolerance [35], due to its performance in validating transactions and the small expected number of malicious actors involved in the network. In summary, this mechanism will consist of three main stages:

1) Proposal phase: A member proposes a block
2) A pre-determined number of consortium members validate the block. The block moves to the next phase if a supermajority (e.g., 2/3) agrees.
3) All organizations update their local copy of the blockchain.

**Smart Contract Management -** The whole process is ruled by smart contracts, ensuring adherence to the judicial process and proper chain of custody. Only primary entities have the right to deploy new versions of smart contracts.

Any member can execute a new smart contract, which will go to its initial stage of the process, however only the prosecution team will have sufficient privileges to promote any new artifact to evidence and under its custody.

The primary entities can only terminate a smart contract, which will be permanently stored in the blockchain for transparency and accountability reasons.

**Access control -** All members in the consortium have read access to the blockchain, however some parts of the blockchain, including block specific data, will not be available to them, depending on the privileges each one has. They can also propose and add new blocks.

**Dispute resolution -** In the event of disputes that impact the functioning of the MTB, the primary entities will have a key role in its resolution, particularly if those arise from secondary entities. Should the dispute arise between the prosecution and the Court chambers, elected representatives from the state parties decide on how to settle the dispute.

**Upgrades and Forks -** Protocol Upgrades to the MTB are proposed jointly by the primary organizations and require a majority consensus from all consortium members.

In the unlikely event of a fork, the chain supported by the primary organizations is considered legitimate.

**Audits and compliance -** Ensuring the compliance of the MTB with legal standards is paramount; therefore, regular audits should be conducted and mandated by the ASP to guarantee the integrity of the blockchain and smart contracts.

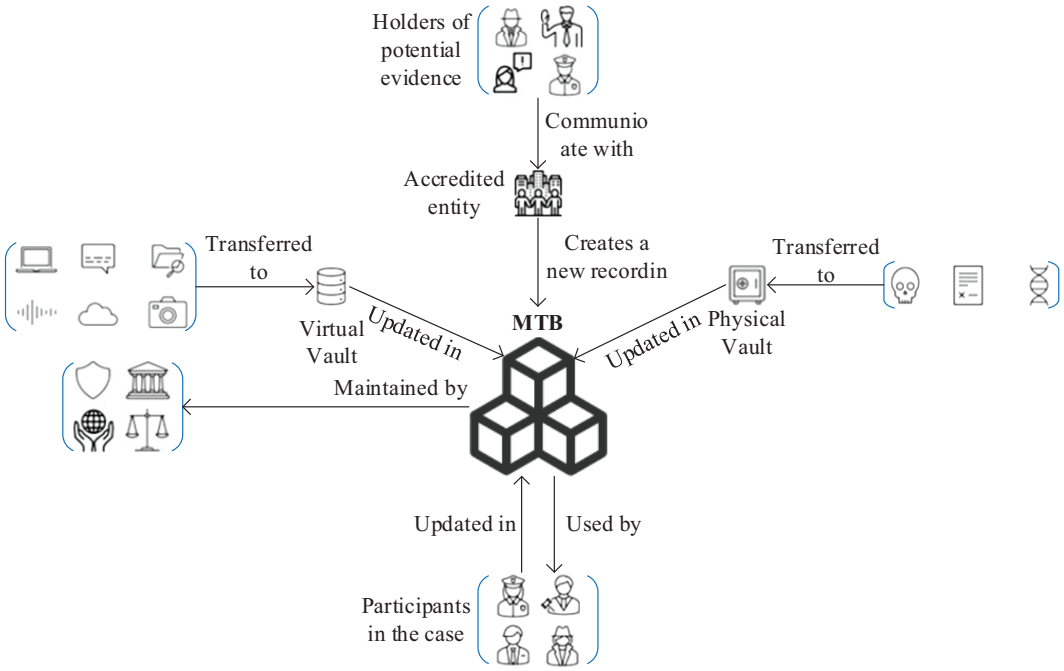


***Figure 6.*** - High level view of MTB

**Evidence Records State lifecycle -** As depicted in Figure 7, with the progress in the judicial process, from non-existent to appeals and reparations, the evidence evolves through different states, according to its validity as evidence within a specific case. The major lifecycle states from evidence are:

1. *Pre-Artifact Creation:* Before an artifact is formally recognized and documented within the ICC's system, the potential evidence or information resides externally.
2. *Artifact Created:* This is the inception point where a piece of evidence or an artifact is first identified and documented as such.
3. *Submitted for Prosecution Review:* The artifact, is presented for preliminary assessment by the prosecution team, determining its relevance to the case.
4. *Pending Review:* The evidence is under active scrutiny by the prosecution. It's being evaluated for authenticity, relevance and overall value to the proceedings.

5. *Approved - Pending Transfer:* The evidence has been deemed valuable and relevant by the prosecution and is awaiting transfer to the next process phase.
6. *Rejected:* Evidence that does not meet the necessary criteria or is deemed irrelevant to the case is rejected at this stage.
7. *In Prosecution's Custody:* The approved evidence is now formally in the custody of the prosecution and is ready for further analysis, presentation or other relevant activities.
8. *In Utilization:* This stage signifies the active use of the evidence in the legal proceedings, be it investigations, pre-trial hearings or main trial sessions.
9. *Archived (from Prosecution):* Post utilization, if the evidence is not immediately required, it is archived for potential future use or reference.
10. *Submitted to the Judiciary:* Evidence that needs to be presented before the judicial chambers is submitted for their review and consideration.
11. *Evidence in Judiciary Custody:* The evidence is now under the formal custody of the judicial chambers, indicating its active consideration in judicial deliberations.
12. *Disclosed to Parties:* Relevant evidence is disclosed to all involved parties, ensuring transparency and adherence to the principles of a fair trial.
13. *Retained:* Post-disclosure, evidence is retained for a specified duration.
14. *Archived (from Retained):* After the retention period, the evidence is moved to long-term storage, ensuring it remains accessible for any future suitable purposes.
15. *Disposed:* The final stage where evidence, after serving its purpose and being archived, is either returned, destroyed or permanently archived based on its nature and the policies of the ICC.

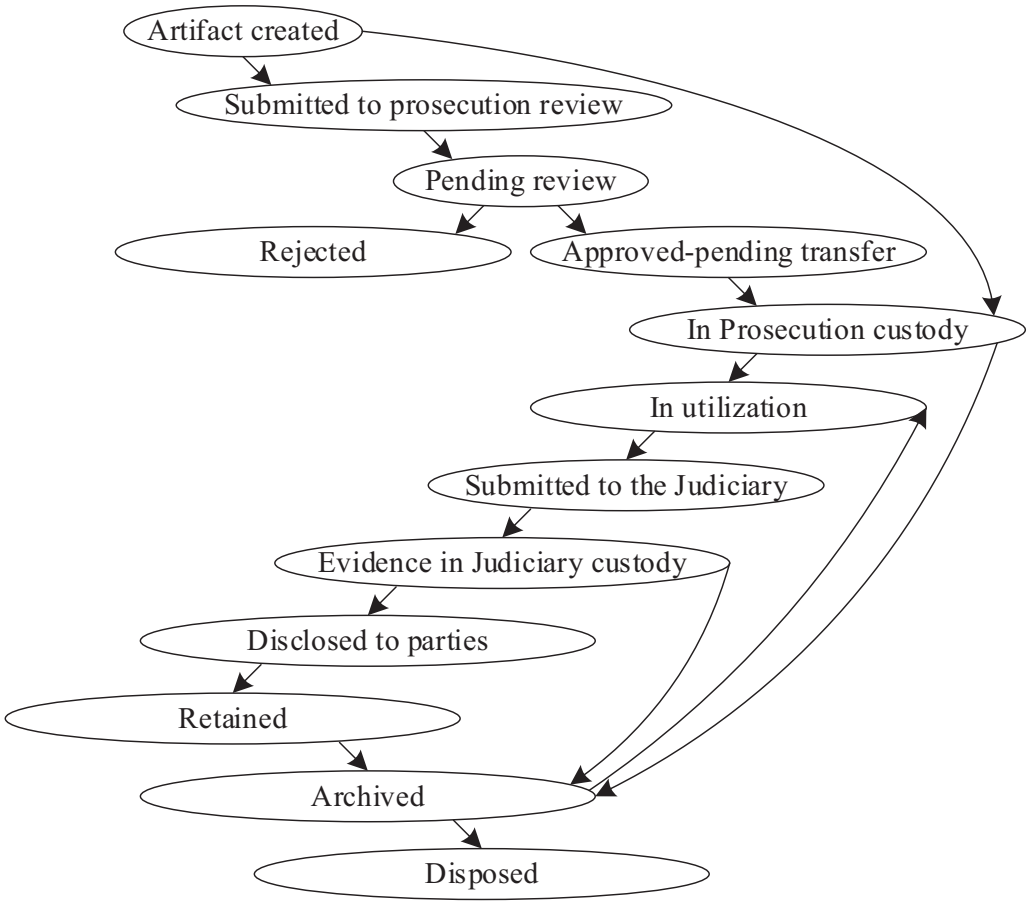


***Figure 7.*** - Evidence Lifecycle stages

## 7 Artifact evaluation

The MTB framework was presented individually to each of the three panel members introduced in section 1.4 during the month of November 2023. It consisted of a meeting to explain the framework and how it could meet the requirements set, followed by a Q&A section. After the meeting, a survey was sent for the evaluation of each participant. The survey questions consisted of the objective statements

presented previously in **Table 1**, instantiated from the DSRM Evaluation Framework. **Table 4** presents the results based on an average of the three respondents. All participants strongly agreed that the framework "Meets the principles of robust evidence management and chain of custody". For all other questions, at least one expert strongly agreed with the statements. On average they were all between agreement or strong agreement, leading to the conclusion that the framework as an artifact fully meets the goals it was intended to do.

***Table 4.*** - Results of panel evaluation survey

| Dimension | Criteria | Average score |
|---|---|---|
| **Goal** | Validity | 5,00 |
| **Environment** | Consistency with organization / utility | 4,33 |
| **Environment** | Consistency with technology / harnessing of recent technologies | 4,33 |
| **Structure** | Completeness | 4,67 |
| **Activity** | Accuracy | 4,33 |
| **Evolution** | Robustness | 4,33 |

## *7.1 Additional evaluation*

With the evaluation of the artifact by the panel of experts, it was decided to expand the evaluation to more participants that weren't directly consulted in the definition and execution of the artifact, to have a more representative and possibly unbiased evaluation of this artifact. As such, another survey was made to an expanded set of participants to have a second degree of evaluation of the artifact.

A total of 30 people that were working or had familiarity with the ICC were invited to participate in this survey which were of the same questions as the ones answered by the panel and had supporting material explaining the MTB framework and the author's contact for any clarification that could be required. With a total population of about 1500 staff and external people, the survey was filled in by 17 people, slightly over 1% of the total population. In order to get a diverse set of viewpoints on this topic, the selected sample tried to represent as much as possible all the major areas of the organization, with a smaller majority working within the information technology sector.

Due to their personal and professional profile, the people selected in the survey were considered a good sounding board for this topic.

**Demographic profile -** The sample consisted of 17 respondents, 76% were male and an average age of 44,7 years. The median age of the participants was 43 years. The standard deviation was 8,41 years, which means that there was relatively low variation in the ages of the participants of the survey.

An important aspect that was not formally measured, nor directly considered, also due to the confidentiality of the participants, was their nationality. However, it is relevant to highlight the high level of diversity in this regard, since there were, out of the 30 people requested to fill in this survey, 20 unique nationalities in this sample. The same applies to the Ethnicity/Race factor, that despite not being formally measured included a wide range of backgrounds.

**Professional profile -** The survey respondents had an average and median professional experience of 20 years. The average tenure at the organization was of over 11 years. However, the median was lower, at 8 years. Additionally, 53% of the respondents had a managerial role.

While not mandatory for non-managerial roles, the large majority of the surveyed people are expected to have a level of studies of at least a bachelors. The employees surveyed were all at intermediate or senior levels of their careers.

For the purpose of this research, and keeping a balance between clarity and the confidentiality of the participants, the survey respondents were divided in two major categories: 1) Legal and judicial administrative teams: Focused on the judicial process of the organization and most have a concentration in legal affairs. This knowledge enables them to be a direct actor, or if indirect, to ensure the judicial process runs smoothly and within the framework of its mandate. Their interaction with information and digital technologies is from an end user perspective. Seven individuals (41%) within this category responded to the survey; 2) Information Technology (IT): People who work daily within the IT environment, ensuring the organization has the right technological tools and to maintain them in

good order to support the judicial process. The focus of this group is in technological aspects and the understanding of legal affairs within the context of the mandate of the organization is superficial in most situations. There were 10 individuals (59%) within this category that responded to the survey. The results discussed consider the two categories combined.

## *7.2 Results*

The results coming from the extended evaluation survey didn't differ too much from the one taken by the panel of experts. On average, there is agreement and strong agreement that the MTB framework would meet the artifact evaluation objectives set.

**Table 5** presents the average results from the extended user evaluation survey.

***Table 5.*** - Results of user sample evaluation survey

| Dimension | Criteria | Average score |
|---|---|---|
| **Goal** | Validity | 4,59 |
| **Environment** | Consistency with organization / utility | 4,59 |
| **Environment** | Consistency with technology / harnessing of recent technologies | 4,06 |
| **Structure** | Completeness | 4,71 |
| **Activity** | Accuracy | 4,47 |
| **Evolution** | Robustness | 4,47 |

Figure 8 displays a graphical representation through a radial chart of the two evaluations, which clearly shows strong agreement, on average, from all participant groups that the MTB fulfils the goals it was set to achieve.

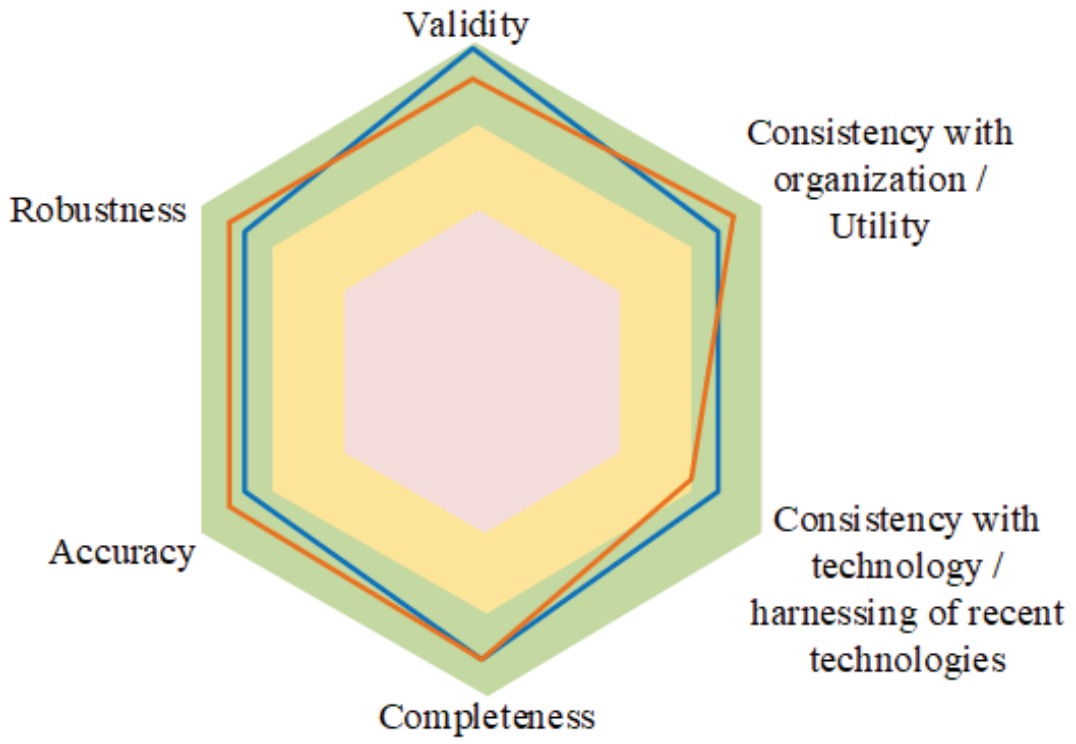


***Figure 8.*** - Evaluation comparison per criteria

## 8 Conclusions

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 ICC, 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 research 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; 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 MTB 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 a solution.

The sixth and final stage – communication, validated the novelty of this research by having its core contributions materialized in the approval of two papers in the conference IBICA 2023.

### *8.1 Components review*

**Blue Ocean Strategy -** On the component of Blue Ocean Strategy, while this being a framework originally aimed at the private competitive sector, it was very enlightening to understand how blockchain technology could help improve the evidence management process by providing more credibility, assurance, and scalability to an area that is usually very manual and cumbersome, such as that the evidence was not tampered with and is authentic.

The tools provided by this framework enabled the validation of blockchain as a technology to manage evidence with the specificities of an organization such as the ICC. It culminated with the validation that the Blue Ocean Strategy criteria fitted with the solution being considered and that there was considerable value to be achieved.

**Literature review -** The literature analyzed confirmed that blockchain is a valid solution for chain of custody and evidence management, however, no study was found that considered the international criminal justice sector and its specificities.

Blockchain as a technology is a relatively new area, and blockchain within the area of chain of custody is more novel. Using the PRISMA methodology and focusing on five key attributes of this research, it was clear that while some papers covered some areas, no paper within the academic literature covered the five key attributes considered here: 1) Blockchain, 2) chain of custody, 3) evidence management, 4) multi-level trust and the 5) public sector.

Concluding that there was a gap in the literature that would encompass all these areas, the need for the consideration for a blockchain-based framework was clear.

**MultiTrustBloc** (MTB) **Framework -** This research concludes with the MTB framework, which provides a design for a blockchain-based system that would enable the ICC to democratize the process of evidence gathering and sharing with higher assurances of authenticity and non-tampering of potential evidence.

A set of techniques was used to define the framework and allow the reader a more concrete understanding of this solution and how it could be built. It establishes the roles in the system, the process flow and the lifecycle of evidence management, from pre-acquisition to archival and removal are considered and defined. Also, and importantly, the main policies of the blockchain solution are chosen and considered on their merits for this solution. The solution assumes a concrete and more tangible perspective with the development of the mockups that could be implemented to produce this solution as an application.

**Evaluation and final considerations -** The initial guidelines of this research and subsequent results were presented and explained to a panel of experts which have agreed on the evaluation parameters and assessed it based on a set of previously defined criteria.

Having analyzed the created artifact, in particular, the MTB framework, the panel of experts generally concluded that the artifact, as it was conceived and developed, fully met the criteria for an evidence management system to be used in an institution such as the ICC.

## *8.2 Future work*

This research lays the foundation of what a blockchain-based evidence management system can be and how it can be designed to fulfill the needs of an institution with a similar mandate as the ICC. Notwithstanding, there are still many ways that this research can be taken forward to expand the body of knowledge in this area, these being:

1. Creation of a proof of concept based on the MTB framework.

Rationale: Implement the blockchain as designed in this research to demonstrate from a practical perspective its added value.

2. Study for a mobile phone-based application that guarantees authenticity of data from when they are captured to submission to accredited entity.

Rationale: Shortening or removing the time between the generation of evidence and its logging will dramatically improve the credibility and trust in the evidence presented in the Court.

3. Study the use of motivating factors in the creation of the MTB solution's user interface.

Rationale: Consider factors that could improve user satisfaction in the user of the solution, and understand how these factors could increase adoption

4. Investigate how evidence could be shared between different instances of the MTB.

Rationale: Evidence is sometimes shared between different organizations. By investigating interoperability possibilities, the judicial system would be reinforced by keeping the chain of custody intact.

**References**


[1] Mosweu, O. and Mosweu, T. (2023). 'The influence of archives in conflict resolution: A case study of Botswana and Namibia'. *Afr. J. Libr. Arch. Inf. Sci.,* 33: 1, 23–36.

[2] Houge, A.B. (2023).' Imageries of self: Guilty plea statements in sexual violence cases at the ICTY'. *Int. Crim. Justice Rev.,* 33: 2, 179–196. 10.1177/1057567720982656.

[3] Cogan, J.K. (2000). 'The problem of obtaining evidence for International Criminal Courts'. *Hum. Rights Q.,* 22: 2, 404–427. 10.1353/hrq.2000.0021.

[4] (2011). *Rome Statute of the International Criminal Court,* The Netherlands: International Criminal Court. https://www.icccpi.int/sites/default/files/RSEng.pdf [Accessed 9 June 2023].

[5] (2013). *Rules of Procedure and Evidence,* Second. The Netherlands: International Criminal Court. https://www.icccpi.int/sites/default/files/RulesProcedureEvidenceEng.pdf [Accessed 9 June 2023].

[6] International Criminal Court. About the Court. https://www.icccpi.int/about/the-court [Accessed 10 September 2023].

[7] 'Understanding the ICC', in *Public Information and Outreach Section.* The Netherlands: The Hague. https://www.icc-cpi.int/sites/default/files/Publications/understanding-the-icc.pdf [Accessed 10 September 2023].

[8] Ulbricht, B.R, Moxley, C., Austin, M.D. and Norburg, M.D. (2022). 'Digital eyewitnesses: Using new technologies to authenticate evidence in human rights litigation'. *Stanford Law Review,* vol. 74, pp. 851889, 2022. [Online]. Available: https://review.law.stanford.edu/wpcontent/uploads/sites/3/2022/04/Ulbricht-et-al.-74-Stan.-L.-Rev.-851.pdf

[9] Bernstein, P.A. and Goodman, N. (1981). 'Concurrency control in distributed database systems', *ACM Comput. Surv. CSUR,* 13: 2, 185–221. 10.1145/356842.356846.

[10] Nakamoto, S. 'Bitcoin: A peertopeer electronic cash system'. https://bitcoin.org/bitcoin.pdf [Accessed 9 June 2023].

[11] Ali, V., Norman, A.A., and Azzuhri, S.R.B. (2023). 'Characteristics of blockchain and its relationship with trust'. *IEEE Access,* 11, 15364–15374. 10.1109/ACCESS.2023.3243700.

[12] Meunier, S. (2018). 'Blockchain 101: What is blockchain and how does this revolutionary technology work?. What is blockchain and how does this revolutionary technology work?', in *Transforming Climate Finance and Green Investment with Blockchains,* pp. 23–34. 10.1016/B978-0-12-814447-3.00003-3.

[13] Peffers, K., Tuunanen, T., Rothenberger, M.A., and Chatterjee, S. (2007). 'A design science research methodology for information systems research'. *J. Manag. Inf. Syst.,* 24: 3, 45–77. 10.2753/MIS0742-1222240302.

[14] Hevner, A.R., March, S.T., Park, J. and Ram, S. (2004). 'Design science in information systems research'. *MIS Q.,* 28: 1, 75–105. 10.2307/25148625.

[15] Prat, N., ComynWattiau, I. and Akoka, J. (2014). 'Artifact evaluation in information systems designscience research - A holistic view'. *PACIS 2014 Proc.* https://aisel.aisnet.org/pacis2014/23

[16] Joshi, A., Kale, S., Chandel, S., and Pal, D. (2015). 'Likert scale: Explored and explained'. *Br. J. Appl. Sci. Technol.,* 7, 396–403, 10.9734/BJAST/2015/14975.

[17] Page, M.J. *et al.* (2021). 'The PRISMA 2020 statement: An updated guideline for reporting systematic reviews', *BMJ,* n71. 10.1136/bmj.n71.

[18] Kim, W.C. and Mauborgne, R. (2004) 'Blue Ocean Strategy'. *Harvard Business Review.* https://hbr.org/2004/10/blueoceanstrategy [Accessed 15 June 2023].

[19] Awladthani, F.S., Porkodi, S., Saranya, R. and Pandurengan, V. (2023). 'A systemic literature review of the adoption of Blue Ocean Strategy by small and medium enterprises for sustainable growth'. *J. Sustain. Sci. Manag.,* 18: 2, 197–230. 10.46754/jssm.2023.02.014.

[20] Jindal, P. and Chavan, L. (2023). 'Role of blockchain technology in creating blue ocean strategy for banking products and services', in *Contemporary Studies of Risks in Emerging Technology: Part B,* pp. 169–182. 10.1108/978-1-80455-566-820231008.

[21] Nasereddin, A.Y. (2023). 'Impact of the Blue Ocean Strategy dimensions in achieving competitive advantage from the perspective of faculty members'. *Inf. Sci. Lett.,* 12: 6, 2685–2698. 10.18576/isl/120639.

[22] Kim, C., Yang, K.H. and Kim, J. (2008). 'A strategy for thirdparty logistics systems: A case analysis using the blue ocean strategy'. *Omega,* 36: 4, 522–534. 10.1016/j.omega.2006.11.011.

[23] Ehrenberg, A.J. and King, J.L. (2020). 'Blockchain in context'. *Inf. Syst. Front.,* 22: 1, 29–35. 10.1007/s10796-019-09946-6.

[24] Olukoya, O. (2021). 'Distilling blockchain requirements for digital investigation platforms'. *J. Inf. Secur. Appl.,* 62. 10.1016/j.jisa.2021.102969.

[25] Khan, A.A., Uddin,M., Shaikh, A.A., Laghari, A.A. and Rajput, A.E. (2021). 'MFLedger: Blockchain hyperledger sawtoothenabled novel and secure multimedia chain of custody forensic investigation architecture'. *IEEE Access,* 9, 103637–103650. 10.1109/ACCESS.2021.3099037.

[26] JaquetChiffelle, D., Casey, E., and Bourquenoud, J. (2020). 'Tamperproof timestamped provenance ledger using blockchain technology'. *FORENSIC Sci. Int.-Digit. Investig.,* 33. 10.1016/j.fsidi.2020.300977.

[27] Liu, G., He. J and Xuan. X (2021). 'A data preservation method based on Blockchain and multidimensional hash for digital forensics'. *Complexity,* 2021. 10.1155/2021/5536326.

[28] Ali, M., Ismail, A., Elgohary, H., Darwish, S. and Mesbah, S. (2022). 'A procedure for tracing chain of custody in digital image forensics: A paradigm based on grey hash and blockchain'. *Symmetry,* 14: 2. 10.3390/sym14020334.

[29] Sathyaprakasan, R., Govindan, P., Alvi, S., Sadath, L., Philip, S. and Singh, N. (2021). 'An implementation of blockchain technology in forensic evidence management', in V. Naranje, B. Singh and S. Velan (eds), *Proc. IEEE Int. Conf. Comput. Intell. Knowl. Econ., ICCIKE,* Institute of Electrical and Electronics Engineers Inc., pp. 208–212. 10.1109/ICCIKE51210.2021.9410791.

[30] Burri, X., Casey, E., Bollé, T. and Jaquet-Chiffelle, D.O. (2020). 'Chronological independently verifiable electronic chain of custody ledger using blockchain technology'. *Forensic Sci. Int. Digit. Investig.,* 33. 10.1016/j.fsidi.2020.300976.

[31] Alruwaili, F.E. (2021). 'CustodyBlock: A distributed chain of custody evidence framework'. *Information,* 12: 2, 88. 10.3390/info12020088.

[32] Kusuma, R.S. (2023). 'Digital evidence security system design using blockchain technology'. *Int. J. Saf. Secur. Eng.,* 13: 1, 159–165. 10.18280/ijsse.130118.

[33] Gopalan, S.H., Suba, S.A., Ashmithashree, C., Gayathri, A. and Jebin Andrews, V. (2019). 'Digital forensics using blockchain'. *Int. J. Recent Technol. Eng.,* 8: 2 Special Issue 11, 182–184.10.35940/ijrte.B1030.0982S1119.

[34] Zhang, Y. Wu, S., Jin, B. and Du, J. (2018) 'A blockchainbased process provenance for cloud forensics', in *IEEE Int. Conf. Comput. Commun.,* ICCC, Institute of Electrical and Electronics Engineers Inc., pp. 2470–2473. 10.1109/CompComm.2017.8322979.

[35] Manjre, B.M. and Goyal, K.K. (2023). 'A novel and custom blockchain approach for the integrity assurance of the digital evidences extracted during the extraction and decoding of mobile artifacts from the mobile forensic tools', in *AIP Conf. Proc.,* American Institute of Physics Inc. 10.1063/5.0127910.

[36] Bonomi, S., Casini, M., and Ciccotelli, C. (2020). 'BCoC: A blockchain-based chain of custody for evidences management in digital forensics', in V. Danos., M. Herlihy, M. PotopButucaru, J. Prat, and S. Tucci-Piergiovanni (eds), *OpenAccess Ser. Informatics,* Schloss Dagstuhl- LeibnizZentrum fur Informatik GmbH, Dagstuhl Publishing. 10.4230/OASIcs.Tokenomics.2019.12.

[37] Yan, W., Shen, J., Cao, Z. and Dong, X. (2020). 'Blockchain based digital evidence chain of custody', in *Proceedings of the 2020 The 2nd International Conference on Blockchain Technology,* in ICBCT'20, New York, NY, USA: Association for Computing Machinery, pp. 19–23. 10.1145/3390566.3391690.

[38] Ahmad, L., Khanji, S., Iqbal, F. and Kamoun, F. (2020). 'Blockchainbased chain of custody: Towards real-time tamper-proof evidence management', in *ACM Int. Conf. Proc. Ser.,* Association for Computing Machinery. doi: 10.1145/3407023.3409199.

[39] Chopade, M., Khan, S., Shaikh, U. and Pawar, R. (2019). 'Digital forensics: Maintaining chain of custody using blockchain', in *Proc. Int. Conf. ISMAC IoT Soc., Mob., Anal. Cloud, ISMAC,* Institute of Electrical and Electronics Engineers Inc., pp. 744–747. 10.1109/ISMAC47947.2019.9032693.

[40] Lone, A.H. and Mir, R.N. (2019). 'Forensicchain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer'. *Digit. Investig.,* 28, 44–55. 10.1016/j.diin.2019.01.002.

[41] Santamaria, P., Tobarra, L., Pastor-Vargas, R. and Robles-Gomez, A. 'Smart contracts for managing the chain-of-custody of digital evidence: A practical case of study'. *SMART CITIES,* 6: 2, 709–727. 10.3390/smartcities6020034.

[42] AwusonDavid, K., AlHadhrami, T., Alazab, M., Shah, N. and Shalaginov, A. (2021). 'BCFL logging: An approach to acquire and preserve admissible digital forensics evidence in cloud ecosystem'. *Future Gener. Comput. Syst.,* 122, 1–13. 10.1016/j.future.2021.03.001.

[43] AlKhateeb, H., Epiphaniou, G. and Daly, H. (2019). 'Blockchain for modern digital forensics: The chain-of-custody as a distributed ledger' in *Adv. Sci. Tech. Sec. Appl.,* Springer, pp. 149–168. doi: 10.1007/9783030112899_7.

[44] Li, M., Lal, C., Conti, M. and Hu, D. (2022). 'LEChain: A blockchainbased lawful evidence management scheme for digital forensic', *Future Gener. Comput. Syst.- Int. J. Escience,* 115, 406–420.10.1016/j.future.2020.09.038.

[45] Shahaab, A., Hewage, C. and Khan, I. (2021). 'Preventing spoliation of evidence with blockchain: A Perspective from South Asia', in *2021 The 3rd International Conference on Blockchain Technology,* in ICBCT '21, New York, NY, USA: Association for Computing Machinery, pp. 45–52. 10.1145/3460537.3460550.

[46] Tsai, F.-C. - (2021). 'The application of blockchain of custody in criminal investigation process', in J. Watrobski, W. Salabun, C. Toro, C. Zanni-Merk, R.J. Howlett and L.C. Jain, (eds), *Knowledge-Based and Intelligent Information & Engineering Systems (kse 2021),* Amsterdam, The Netherlands: Elsevier Science Bv, pp. 2779–2788. 10.1016/j.procs.2021.09.048.

[47] Sanda, P., Pawar, D. and Radha, V. (2022). 'Blockchain-based tamper-proof and transparent investigation model for cloud VMs'. *J. Supercomput.,* 78: 16, 17891–17919. 10.1007/s11227-022-04567-4.

[48] Akello, P., Vemprala, N., Lang Beebe, N. and Raymond Choo, K.K. (2023). 'Blockchain use case in ballistics and crime gun tracing and intelligence: Toward overcoming gun violence'. *ACM Trans. Manag. Inf. Syst.,* 14: 1, 7:1–7:26. 10.1145/3571290.

[49] Martin, T. and Hammoudeh, M. (2022).'"Data preservation system using BoCA: Block-chain-of-custody application', in *The 5th International Conference on Future Networks & Distributed Systems,* in ICFNDS 2021, New York, NY, USA: Association for Computing Machinery, pp. 70–77. 10.1145/3508072.3508084.