iscte
INSTITUTO
UNIVERSITÁRIO
DE LISBOA

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

Nuno Miguel Barranha Rodrigues dos Santos

Master's in Digital Technologies for Business

Supervisors:
Doctor João Carlos Ferreira, Assistant Professor with aggregation,
ISCTE, University Institute of Lisbon

Joel Curado Silveirinha, Invited Assistant
ISCTE, University Institute of Lisbon

December 2023

iscte

TECNOLOGIAS
E ARQUITETURA

Departamento de Ciências e Tecnologias da Informação

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

Nuno Miguel Barranha Rodrigues dos Santos

Master's in Digital Technologies for Business

Supervisors:
Doctor João Carlos Ferreira, Assistant Professor with aggregation,
ISCTE, University Institute of Lisbon

Joel Curado Silveirinha, Invited Assistant
ISCTE, University Institute of Lisbon

December 2023

Acknowledgements

This dissertation is the culmination of one year of intense academic work, where I have learned so much and rediscovered the pleasure for the academic life, including lectures, research, and writing. I'm grateful to ISCTE, the place that saw me graduate in 2008 and that once again, contributed to my development by welcoming me to this master's degree.

A special thank you to Professor João Carlos Ferreira, the coordinator of the master's and primary supervisor of this dissertation for being readily available to guide me whenever Also thank you to Professor Rubén Pereira for his captivating lectures and continuous food for thought.

Throughout this academic path I learned so much with so many people, from fellow students to lecturers, but two colleagues gained a special place in my memories: Doroteia Serrão, for her genuine happiness, energy, and business acumen; and Pedro Nascimento for his perfectionism, attention to detail, and eagerness to help others. Our joint work assignments not only were very successful, but they were as demanding as they were fun!

To my parents, which have supported me throughout my development as a person and as a professional, and dared to visit me wherever my career has taken me.

To my lovely wife and son, who inspire me daily to become a better person. I couldn't do this without your support. The many and long hours of research and writing for this dissertation could have taken a toll on our family, but thanks to your love and care I had the stability to persevere until the end and produce something that I'm proud of.

At last, but not least, thank you, the reader of this dissertation, for investing your time in reading the result of a year of intense research and writing. I sincerely hope this helps you in using blockchain technology for good, such as for the benefit of (inter)national public service.

There can be no peace without justice, no justice without law and no meaningful law without a Court to decide what is just and lawful under any given circumstance.

– Benjamin Ferencz

Abstract

International Criminal Courts are a guarantor that justice can be achieved for the most egregious crimes against humanity and that surviving victims from those crimes can live with the assurance that the perpetrators are 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 International Criminal Courts 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, cyber-threats, size and complexity of evidence, traditional methods of managing the chain of custody are becoming vulnerable to the successful challenging of 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 dissertation conceives and designs a blockchain-based framework that maintains a tamper-proof 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

Resumo

Os Tribunais Penais Internacionais são uma garantia de que a justiça pode ser alcançada para os crimes mais graves contra a humanidade e que as vítimas sobreviventes desses crimes podem viver com a certeza que os autores serão responsabilizados pelos seus atos.

Esses crimes são complexos, sensíveis e podem ser utilizados como arma para os objetivos e interesses de intervenientes. Consequentemente, a credibilidade destas instituições é frequentemente atacada, sendo crucial que o processo em que exercem o seu mandato seja rigoroso e eficaz.

As provas estão no centro do processo judicial e os participantes confiam que sejam autênticas, inteiras e não adulteradas para garantir a justiça dos procedimentos. Sem poderes de execução, estes Tribunais Penais Internacionais podem basear-se amplamente em provas fornecidas por outras partes para construir um caso sólido desde o início até à fase de recurso.

Com o aumento da digitalização das provas, as ameaças cibernéticas, a dimensão e a complexidade das provas, os métodos tradicionais de gestão da cadeia de custódia estão a tornar-se vulneráveis à contestação bem-sucedida da admissibilidade das provas.

A Blockchain pode ser a resposta para o reforço da cadeia de custódia na gestão de provas, uma vez que esta tecnologia traz características essenciais como registo temporal, autenticação, imutabilidade e confiança entre partes independentes.

Esta dissertação concebe e projeta um quadro baseado em cadeias de blocos que mantém uma cadeia de custódia inviolável e uma confiança a vários níveis na gestão de provas. Garante a autenticidade e a indiscutibilidade das provas em processos judiciais.

Palavras-chave: Cadeia de Blocos, Cadeia de Custódia, Gestão de Prova, Tribunal, Judicial, Justiça Criminal Internacional, Tribunal Penal Internacional

Table of contents

List of Figures

List of Tables

Abbreviations

ASP	**A**ssembly of **S**tate **P**arties
BPMN	**B**usiness **P**rocess **M**odelling **N**otation
DSRM	**D**esign **S**cience **R**esearch **M**ethodology
ICC	**I**nternational **C**riminal **C**ourt
MTB	**M**ulti**T**rust**B**loc
NGO	**N**on-**G**overnmental **O**rganization
PRISMA	**P**referred **R**eporting **I**tems for **S**ystematic **R**eviews and **M**eta-**A**nalyses
PoW	**P**roof **o**f **W**ork
Q&A	**Q**uestions **a**nd **A**nswers

CHAPTER 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 inter-national 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, 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, Defence and the Court's Registry in managing evidence properly since collection until disclosure [3].

Every single International Criminal Court 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 the chain of custody remained intact.

The motivation behind this dissertation 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, 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 analysed 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 outcome 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 International Criminal Court, headquartered in The Hague, as a basis for this dissertation, 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

In today's society, 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 achievement 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 study conducted for this dissertation 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 International Criminal Court’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 International Criminal Court (ICC) is an important institution in the realm of international justice. Established as the world's first permanent international criminal court, 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 these 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.

Its key characteristics are:

- Judicial Proceedings: The ICC ensures that trials are fair, and its judges are responsible for overseeing the fairness of the proceedings.
- Independent Prosecution: The Office of the Prosecutor operates as an independent organ of the Court. This office conducts preliminary examinations, investigations, and is solely responsible for bringing cases before the Court.
- Defendants' Rights: Every defendant is entitled to public, fair proceedings in a language they fully comprehend.
- Victims' Participation: The Rome Statute grants victims unprecedented rights to participate in ICC proceedings.
- Protection for Victims and Witnesses: The ICC has established a protection program for victims and witnesses, incorporating both operational and procedural protective measures.
- Outreach: The Court actively engages in dialogue with communities affected by the crimes under its jurisdiction. This engagement allows these communities to communicate directly with the Court and fosters a sense of ownership in the judicial process.

ICC's Judicial Proceedings:

The judicial proceedings of the International Criminal Court (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:
   a. *Proprio Motu*: The Prosecutor can initiate an investigation on their own accord based on information received from individuals, organizations, or other sources.
   b. Referral by a State Party: A member state of the Rome Statute can refer a situation to the Prosecutor.
   c. Referral by the United Nations Security Council: The UN Security Council can refer a situation to the ICC, irrespective of whether the concerned state is a party to the Rome Statute or not.
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 defence 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 defence 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 this evidence remains authentic and valid to be assessed by the Judges' Chamber.

Other 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 followed 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, expert report, among other types. All others in which the content cannot be recorded and stored digitally, at a minimum require a digital record that they exist and are classified as evidence, even if they are accessible in another place than a digital platform or physical format.

As mentioned previously, an important aspect of evidence management is the chain of custody, and the ability from 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 decentralized validation of state and transactions, and thus allowing for the interaction of different actors that do not necessarily trust each other but that 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.

Within the scope of this dissertation, and as discussed before, trust is critical to ensure the success of a Blockchain based evidence management platform. Figure 1 depicts the most important characteristics for trust in a Blockchain solution, which coincide the characteristics of a successful evidence management platform.

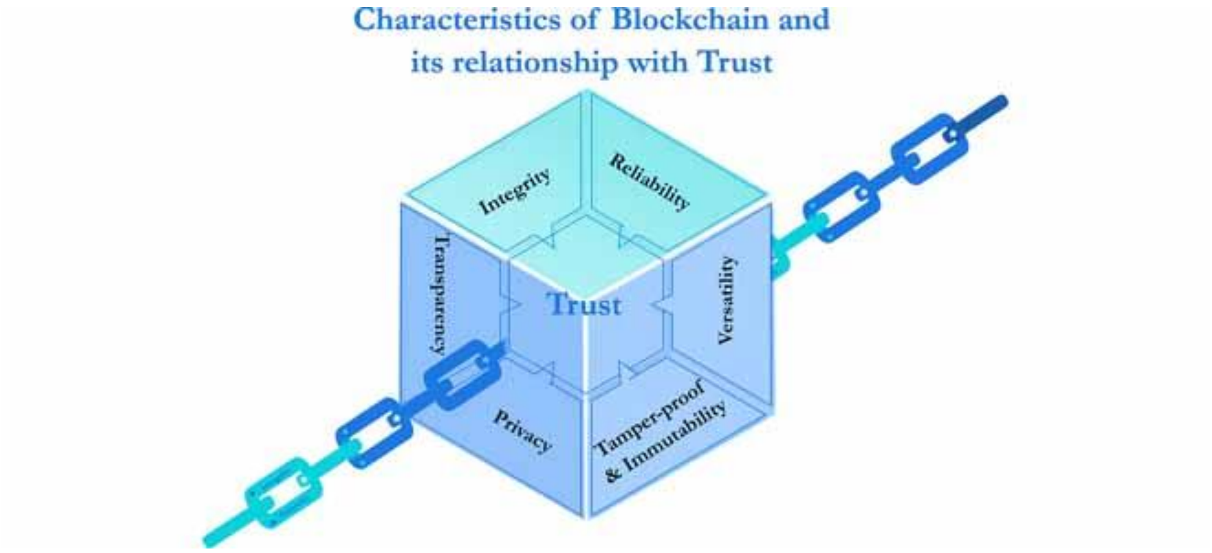

Characteristics of Blockchain and its relationship with Trust
Integrity
Reliability
Transparency
Trust
Versatility
Privacy
Tamper-proof & Immutability

Figure 1 - Characteristics of Blockchain and its relationship with Trust [11]

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 behavioural science, which seeks to formulate theories predicting individual and organizational behaviour. The second paradigm, design-science, focuses on enhancing the capabilities of individuals and organizations by creating innovative artifacts [14].

In this context, this dissertation 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, depicted in Figure 2.

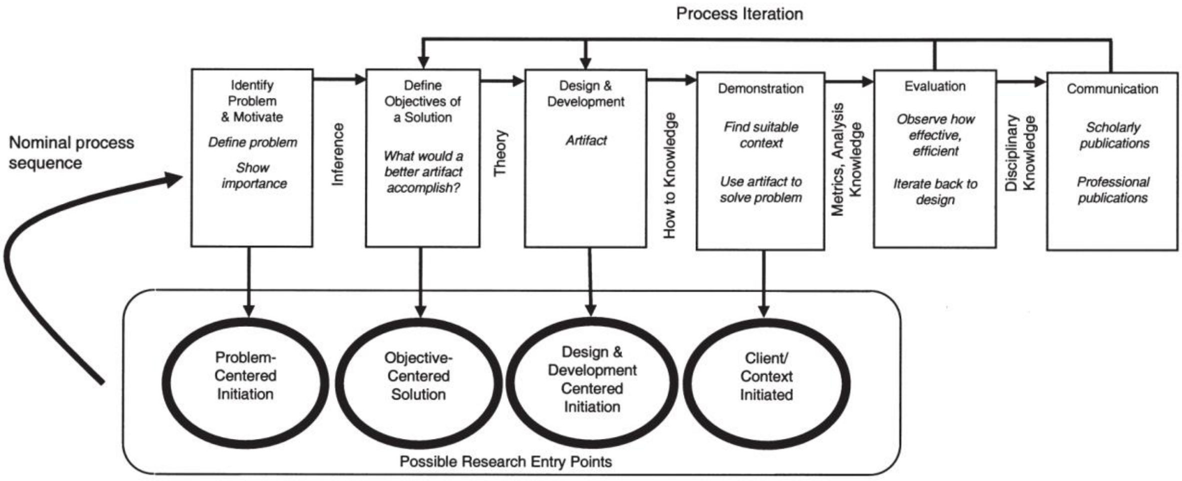

Process Iteration
Nominal process sequence
Identify Problem & Motivate
Define problem
Show importance
Inference
Define Objectives of a Solution
What would a better artifact accomplish?
Theory
Design & Development
Artifact
How to Knowledge
Demonstration
Find suitable context
Use artifact to solve problem
Metrics, Analysis Knowledge
Evaluation
Observe how effective, efficient
Iterate back to design
Disciplinary Knowledge
Communication
Scholarly publications
Professional publications
Problem-Centered Initiation
Objective-Centered Solution
Design & Development Centered Initiation
Client/ Context Initiated
Possible Research Entry Points

Figure 2 - DSRM framework [13]

The artifact to be created in this dissertation is the creation of a conceptual framework, denominated as MultiTrustBloc. It has a problem centred initiation, and it aims to follow all the steps until communication stage.

An important part of validating the output of such method was to assemble a panel of experts that would validate the problem and evaluate the artifacts. The panel consisted of three individuals that combined have decades of experience in International Criminal Courts. 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 which have: a combined amounts of relevant experience of over 35 years; 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, being one an IT specialist, another a legal specialist in victims and witnesses, and the third one had several years in Prosecution side.

An initial meeting was held in the month of June 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].

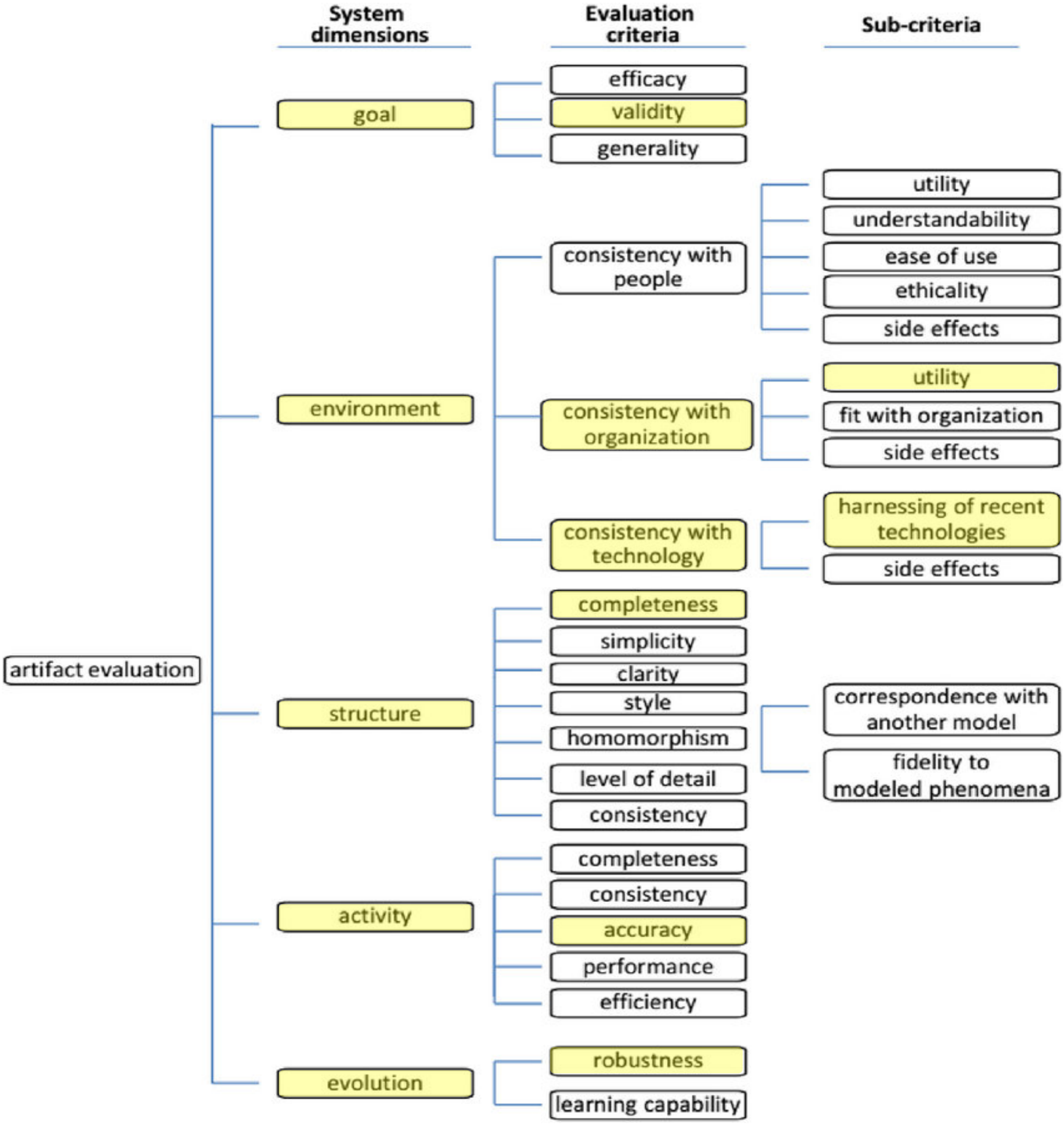


Figure 3 – DSRM artifact evaluation framework with selected criteria highlighted. Updated from [15]

For the evaluation of the created framework, the previously described panel of specialists provided their expert knowledge by validating the solution presented in this dissertation. The artifact was measured based on the following objectives:

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.

Through a survey, these specialists evaluated the framework based on the evaluation criteria set in Figure 3, 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 “Strongly agree”.

1.5. Overview of the dissertation

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 dissertation. 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: Related work. It makes use of the PRISMA [17] methodology to perform a systematic literature review on the topics covered this dissertation, including a comparative analysis of five dimensions, namely: Blockchain, Chain of Custody, Evidence Management, Multi-level trust, 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 dissertation.

CHAPTER 2

Blue Ocean Strategy analysis

2.1. Motivation for using Blue Ocean Strategy

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

Bringing the value and innovation mindset of the Blue Ocean Strategy to the International Criminal Justice system was considered relevant to understand how a blockchain based solution could reinvent the evidence management process and systems that currently support the chain of custody and credibility of these public institutions.

The use of this strategy methodology could help identify more accurately if blockchain technology could be a value add to the evidence management process within the public sector, particularly the judicial one.

As this strategy originally focused on private and competitive sector, it was important to understand if others had already considered this approach within the scope of this dissertation.

2.2. Identification of current body of knowledge

A search for Blue Ocean Strategy applied to judicial system was done in 3 databases (Scopus, ACM Digital Library and IEEE) on the 11th of October 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 database and having looked at the title of each one of them, none referred, direct or indirect, to the judicial sector, as the results only arose from a combination of the first term with the word evidence. Alternatively, only one result was returned when using the following string [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 already been researched in a broad range of areas, such as 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 well-defined mandate and mutually exclusive, the origination of this type of strategy focuses on their evidence management capabilities from a general perspective. The consideration of reducing competition is therefore not considered, and the objective is consequently on the value added that such solution can bring to the sector.

2.3. Strategy Canvas approach

The identification of major characteristics of current judicial evidence management systems was done as well as 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. The factors considered were:

Eliminate

Reliance on controlling party for evidence integrity: it reflects the situation that evidence is at the mercy of the party who controls it. Only when the evidence is disclosed, other parties can guarantee the immutability of the evidence and they will have different copies of the same evidence.

MultiTrustBloc 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, disclosure, and presentation in Court, it is often required at least a witness to validate the veracity of evidence being presented in Court. Additionally, the relative easiness to tamper with the data requires a third party, for example a witness, to validate the evidence authenticity.

MultiTrustBloc: 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 when 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 low visibility and higher chance than desired that evidence could be adulterated.

MultiTrustBloc: 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, 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.

MultiTrustBloc: 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 it read the same file directly without having each one a different place they 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.

MultiTrustBloc: 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 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 register, perform its due diligence to minimize any possibility the evidence is not authentic or invalid in Court. For each piece or batch of evidence received, it requires processing it from the very beginning.

MultiTrustBloc: 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 court 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.

MultiTrustBloc: 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 can have a bigger impact in the fulfilling of 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 is linkage could easily break due to human error or outsider’s action.

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

MultiTrustBloc: 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.

2.4. 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 4 depicts how MultiTrustBloc compares with the incumbent evidence management solution.

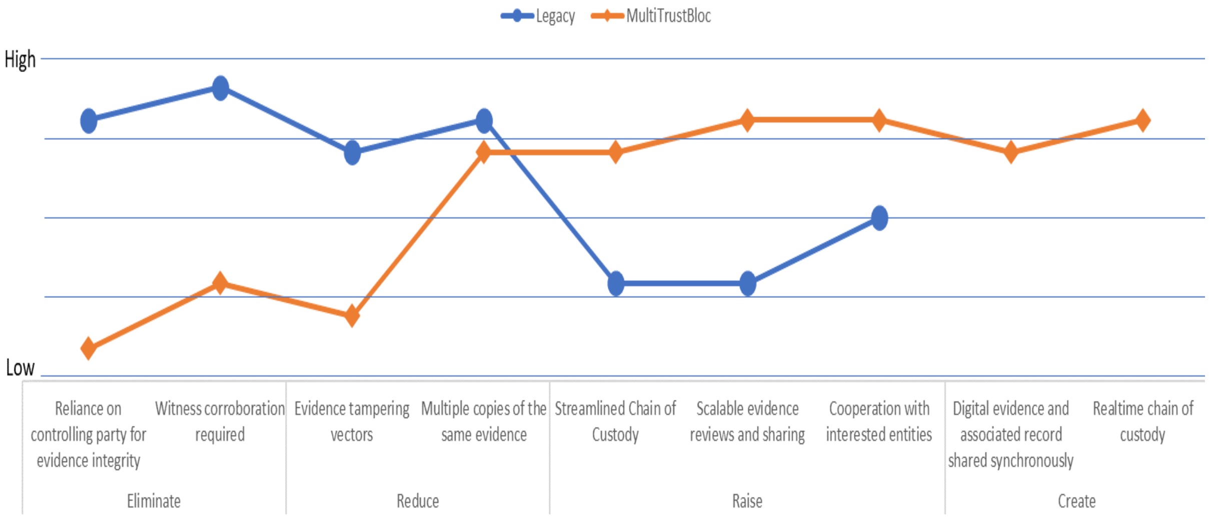


Figure 4 - Strategy Canvas for current Evidence Management solutions and MultiTrustBloc

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 section compares the MultiTrustBloc with those same requirements:

Creates uncontested market space?

Yes. While international criminal courts don't have competition, by implementing such 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 it pursue the accomplishment of its mandate.

Breaks the value-cost trade-off?

Yes. It becomes a matter of trust and confidence that the data is 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, which can be particularly high.

In conclusion, using the Blue Ocean Strategy approach, namely the Strategy Canvas and other tools within this framework it is possible to conclude that blockchain technology would meet several requirements that current evidence management systems don't and increase trust, protection against tampering, and attacks on evidence integrity.

CHAPTER 3

Related Work

3.1. PRISMA Methodology

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 chain of custody within the legal or investigative area. 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 with which ISCTE has access agreements which, combined, have dozens of millions of articles available for access and research:

- Scopus
- Web of Science
- ACM Digital Library
- IEEE

The databases were accessed on the 22nd of June 2023, and thereafter, a total of 65 documents were screened, after the removal of a total of 41 duplicate records from the databases searched. 12 were not able to be retrieved without incurring additional costs. 8 studies with IoT in the title were removed as they deviate from the purpose of this research.

Once the first screening of studies was concluded, 45 articles were assessed for eligibility. 15 of these had an abstract which was not relevant, and for 3 after analysing 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 5.

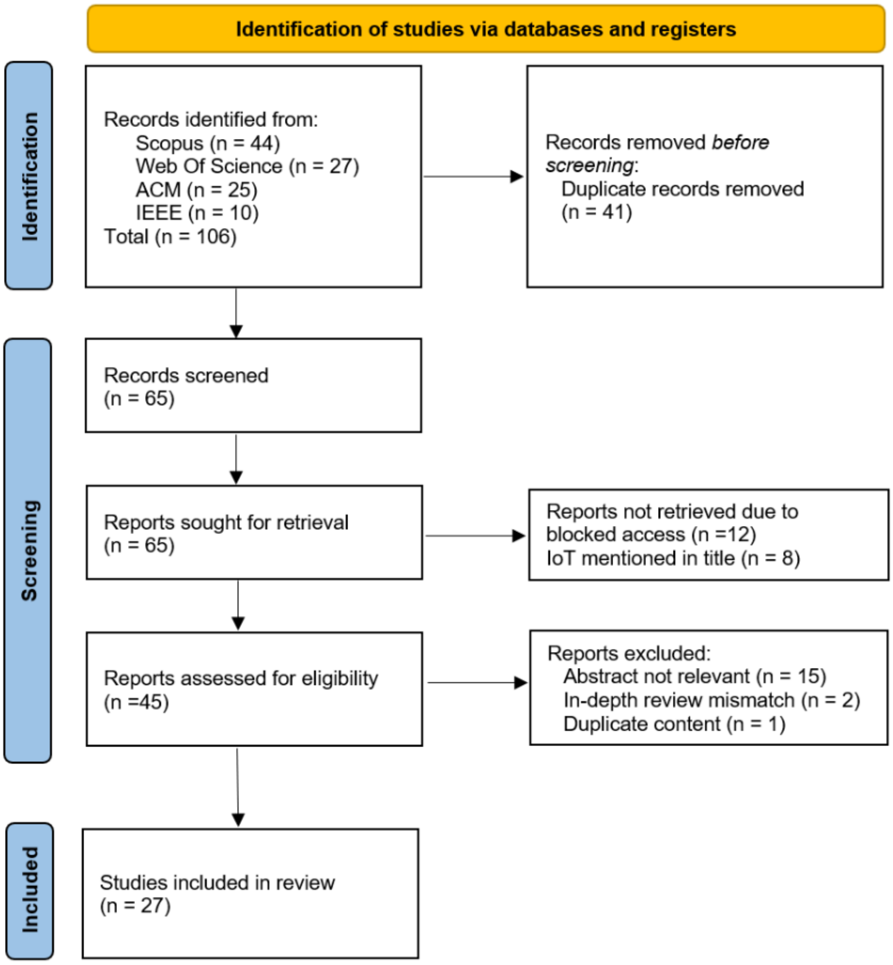

Identification of studies via databases and registers
Identification
Screening
Included
Records identified from:
Scopus (n = 44)
Web Of Science (n = 27)
ACM (n = 25)
IEEE (n = 10)
Total (n = 106)
Records removed *before screening*:
Duplicate records removed
(n = 41)
Records screened
(n = 65)
Reports sought for retrieval
(n = 65)
Reports not retrieved due to
blocked access (n =12)
IoT mentioned in title (n = 8)
Reports assessed for eligibility
(n =45)
Reports excluded:
Abstract not relevant (n = 15)
In-depth review mismatch (n = 2)
Duplicate content (n = 1)
Studies included in review
(n = 27)

Figure 5 - PRIMA instance of the literature review for this dissertation

3.2. Literature review

The literature around this topic is still very nascent, with the first related study being published in 2018. Figure 6 shows an increased interest in this topic, despite the trough that occurred in 2022, with only 3 studies published.

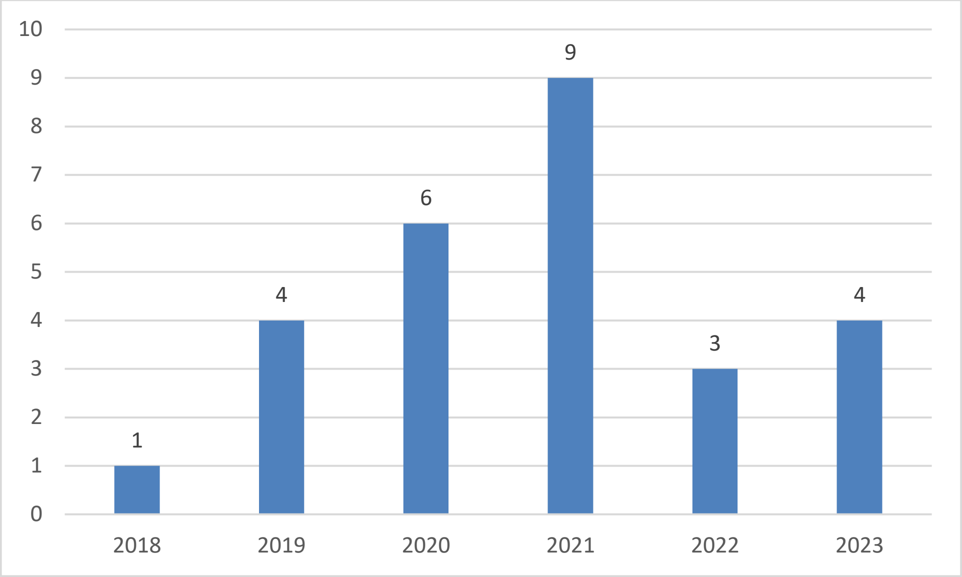


Figure 6 - Number of eligible articles published per year

In this chapter, a variety of articles related to the intersection of blockchain technology and 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?

Once the studies were reviewed, it was possible to group them into these categories, to understand more clearly their focus area on and how it relates to this research.

Group A – Research solely blockchain and Chain of Custody attributes

This group represents research focused solely on the blockchain and chain of custody attributes but does not address the aspects of evidence management, multi-level trust, or public sector applicability. There are 4 such studies.

Given the complex interplay between social systems and technology, the authors of [23] discuss blockchain through a sociotechnical lens. This perspective allows for a more nuanced understanding of the technology, considering not just its technical features, but also its societal implications and potential applications. A major theme in the article is the authors' belief in the significant potential of blockchain around the chain of custody. They highlight that blockchain technology could revolutionize this process due to its inherent characteristics like transparency, security, and immutability. As with any new nascent technology, it is very hard to predict the path blockchain will take. By proposing a learning-by-doing approach, the authors underline the importance of practical, hands-on experience in exploring and understanding blockchain's capabilities and limitations. They believe that actual application and experimentation can pave the way for significant advancements in this field.

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 wherein blockchain technology is used to ensure the authenticity and immutability of forensic findings and subsequent analysis actions. This approach aims to address some of the challenges faced in digital investigations, such as data tampering and lack of traceability and is a novel approach to enhance the reliability and integrity of digital investigations. The stored data on the blockchain, being immutable and verifiable, provides 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. Once consensus is achieved, the data is securely stored on the blockchain ledger, thus ensuring its immutability and verifiability. The authors argue that this enhances the security and efficiency of multimedia investigations, thereby addressing 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 and capable of supporting automation, standardization, and interoperability. The authors highlight the feature that allows the data originator to create a permanent proof via a web browser, demonstrating that he or she 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 multi-level trust nor the public sector

This group includes research that not only addresses blockchain and Chain of Custody attributes, but also incorporates evidence management. These studies, however, do not cover multi-level trust or public sector implications. There are 7 studies under this category.

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. This model aims to provide a solution to the current predicament in digital forensics: proving the originality and validity of digital data. 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. Their proposed procedure highlights the importance of a secure and tamper-proof method of tracking the history and handling of digital evidence - in this case, digital images. 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, offering a way to trace the chain of custody with a high degree of confidence and accuracy.

Sathyaprakasan and co-authors delve into the fundamental concepts of blockchain 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. This would ensure the immutability, traceability, and authenticity of the evidence.

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 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 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, assuring that the evidence has not been tampered with during the investigation process. Additionally, Proof of Work (PoW) consensus algorithm is employed to verify the integrity of the blocks in the blockchain. It adds another layer of security and assures that the evidence within the blocks remains unchanged and authentic.

Group C – Research covering all attributes except 5. Public Sector

This group extends to cover all attributes except public sector considerations, with a total of 8 studies falling into this category.

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 its use as evidence in court. They propose a specially designed blockchain system built from the ground up to fulfil the requirements of preserving digital evidence, ensuring its stored form is immutable and trustworthy.

The authors in [36] explore the potential of utilizing blockchain technology in the management of Chain of Custody, arguing that its inherent characteristics align with the aforementioned CoC requirements. 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 [38], 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, reinforcing the integrity and reliability of the evidence chain of custody.

The article [39] 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:

a) The Evidence Layer: This layer supports a trusted storage medium for digital evidence, ensuring its safety and authenticity.

b) 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.

c) The Network Layer: This layer provides peer-to-peer (P2P) connectivity among all parties that come into contact with the evidence. It facilitates communication and cooperation between different stakeholders, such as forensic investigators, law enforcement agencies, and court systems.

The article [40] 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:

a) Evidence Creation: The ability to accurately record and store digital evidence securely.
b) Evidence Hash Transfer: The use of cryptographic hash functions to maintain the integrity of digital evidence while it is transferred between different parties.
c) 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. This could have significant implications for legal proceedings where the authenticity and integrity of digital evidence can majorly impact the outcome.

The authors in [41] 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. They propose using blockchain technology to create an immutable record of these transactions, guaranteeing the integrity of the evidence and procedures involved. To validate their concept, Lone and Mir present a proof of concept (PoC) using Hyperledger Composer, an open-source development toolset and framework for creating blockchain applications and smart contracts within private networks 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 [36]. It expands on previous work conducted by Bonomi and others [36]. The authors focus on exploring different aspects of the Chain of Custody (CoC) in digital forensics, specifically examining different architectures: centralized, distributed, and multi-blockchain. The benefits and drawbacks of each of these architectures are identified, and the potential of blockchain technology in maintaining the chain of custody for digital evidence is recognized. The authors focus particularly on distributed architecture, which can provide decentralized and tamper-resistant 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 zero-knowledge proof [42], 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 encapsulates studies covering every attribute except multi-level trust, emphasising public sector applicability. There are 5 such studies.

With a focus on log files gathered from a Cloud Service Provider (CSP) [43], the authors identify and analyse the benefits of incorporating blockchain into the process of capturing and maintaining log files in a cloud environment as a way to deliver significant value to the process of digital forensics. They also compare this blockchain-based approach to the conventional methods of collecting and preserving forensic evidence.

In the article [44], 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. They also function as a layer of data replication that further secures and validates the evidence stored in the blockchain.

Another study fitting within this group is called LEChain [45]. It utilizes blockchain technology to supervise the entire flow of evidence as well as all court-related data. It is designed to oversee the entire judicial process, from evidence collection during police investigations to jury voting during court trials. It is a comprehensive management system that allows for greater transparency, accountability, and security throughout the judicial process.

In [46] 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, a crucial feature in fostering an environment of accountability and trust. Additionally, it offers the option for the original uploaders of confidential evidence to disclose it if they believe the involved parties are not acting appropriately.

In [47], Tsai presents an approach to managing evidence within criminal investigations by leveraging the capabilities of blockchain technology, namely the Ethereum [48] platform, supplemented by smart contracts.

Group E – Individual studies which had unique coverage of attributes.

This group represents individual studies with unique coverage of attributes, which may or may not fully incorporate all the attributes. There are 3 studies in this category.

Sanda et al [49] 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 of the article suggest an investigation model that offers a tamper-proof and transparent investigation process for stakeholders involved in examining cloud virtual machines. The authors don't explore how Evidence Management process could be supported in this solution.

Akello et al. [45] investigate the capacity of blockchain technology to tackle gun violence issues, particularly in the context of 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 approach seeks to ensure the traceability and accountability of gun ownership and transactions, potentially contributing to reducing gun-related violence. The focus of the article falls outside of multi-level trust and evidence management.

The authors of [50] propose a data preservation system called BoCA (Blockchain-of-Custody Application), which is compatible with various blockchains, including Ethereum and BitCash. Their solution allows to store data, encrypted or otherwise, in a transparent and verifiable manner.

3.3. Literature review conclusions and gaps identified.

The literature available within this topic clearly demonstrates the increased attention to the value of blockchain to maintain tamperproof chain of custody and to support the management of evidence in 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 analysed approach this subject in different and novel ways.

During the systematic review no study would encompass all five attributes this research touches on, and as such this is a good addition to the body of knowledge within this area. Table 2 depicts the articles, grouped by attribute set and compares them with this research.

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*	*Total*
***A –** Research solely blockchain and Chain of Custody attributes*	Y	Y	N	N	N	4
***B –** Research addresses Evidence management with Chain of Custody on Blockchain, but not multi-level trust nor the public sector*	Y	Y	Y	N	N	7
***C –** Research covering all attributes except 5. Public Sector*	Y	Y	Y	Y	N	8
***D –** Research covering all attributes except 4. Multi-level trust*	Y	Y	Y	N	Y	5
***E –** [49]*	Y	Y	N	Y	Y	1
***E** – [51]*	Y	Y	N	N	Y	1
***E –** [50]*	Y	N	N	N	N	1
This research	**Y**	**Y**	**Y**	**Y**	**Y**	1

CHAPTER 4

MultiTrustBloc Framework

4.1. Objectives of the Solution

As delineated in Chapter 1.1 the ICC could grapple with challenges pertaining to evidence management, particularly in ensuring the sanctity, authenticity, and chain of custody of evidentiary materials. Blockchain technology emerges as a potential panacea to these challenges in the contemporary digital age. This chapter elucidates the objectives of integrating a blockchain solution within the ICC's operational framework, specifically addressing the identified problems.

Ensuring Tamper-Proof Evidence Management

Objective: To establish an immutable and chronological record of evidence, ensuring that once an item is entered into the blockchain, it cannot be altered retroactively.

The decentralized nature of blockchain, coupled with cryptographic hashing, ensures that every piece of evidence, once recorded, becomes an indelible part of the chain. This immutability can significantly reduce the potential for intentional tampering or inadvertent alterations, thereby bolstering the integrity of evidence.

Facilitating Transparent Chain of Custody

Objective: 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.

Blockchain's inherent structure allows for creating a transparent ledger that records every transaction or interaction with a piece of evidence. This ensures that every stakeholder, from investigators to prosecutors, leaves a traceable footprint, reinforcing the chain of custody and reducing ambiguities in evidence handling.

Streamlining Collaboration with Third Parties

Objective: 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.

By utilizing smart contracts and permissioned blockchain structures, the ICC can facilitate controlled access to external entities, allowing them to contribute evidence directly to the blockchain. This expedites the evidence-sharing process and ensures that the evidence remains pristine and unaltered during the transition.

Enhancing Verification and Authentication Processes

Objective: To speed up evidence verification, ensuring rapid yet robust authentication mechanisms. Blockchain's consensus algorithms, combined with its transparent ledger, can significantly streamline the process of evidence verification. Every piece of evidence can be swiftly cross-referenced against its blockchain entry, ensuring its authenticity, and reducing the time and resources traditionally expended in verification processes.

Bolstering Public Confidence and Accountability

Objective: 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.

The transparent and immutable nature of blockchain can serve as a testament to the ICC's commitment to upholding the highest standards of justice. By allowing controlled public access to the blockchain ledger, the ICC can foster greater trust and confidence in its processes, ensuring that justice is both transparent and accountable.

4.2. System actors identified.

Table 3 identifies the roles and high-level view of permissions people performing them have.

Table 3 – MultiTrustBloc 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 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 individual 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 judgment 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 Defence or Victims representatives may require evidence disclosure to participate in the proceedings.

4.3. Process Flows identified.

Evidence acquisition Process

This process starts in the moment that any party identifies some 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 7, using BPMN [52].

The process instantiation can have multiple starting points, and what differentiates them is the stage of the process they start in.

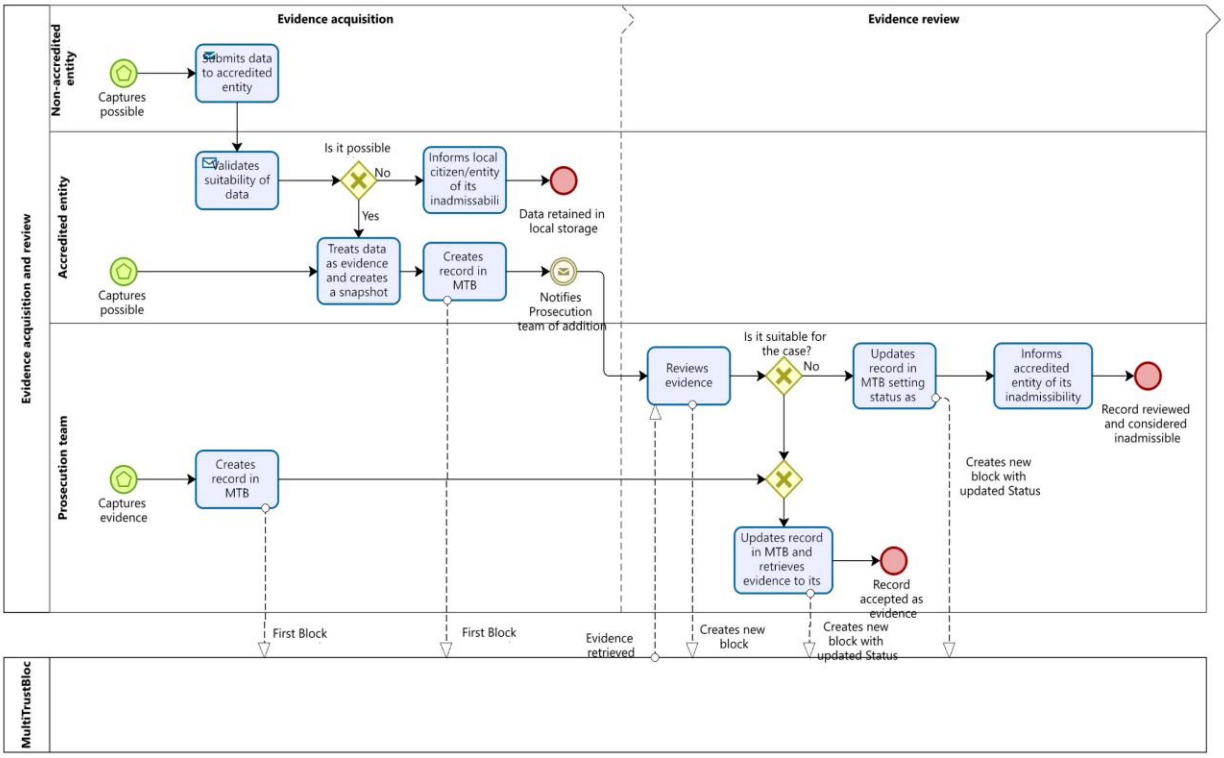
One of the multiple starting points is when a non-accredited entity, either a person individually or through an organization captures data that is considered relevant for any situation that is either active or could potentially be referred to the ICC at a future stage.

1. **Submits data to accredited entity:** The person or organization, holding potential valuable information reaches out to an accredited organization that has direct contact and relationship with the Court.
2. **Validates suitability of data:** When the data is received, the receiver will validate its suitability against ICC's Rome Statute [4] and its rules of procedure and evidence [5].
    a. **Informs local citizen/entity of its inadmissibility:** If the data provided doesn't meet the minimum admissibility threshold, the evaluator will inform the entity that submitted the data, that it cannot be considered as evidence and will not be processed further.
3. **Treats data as evidence and creates snapshot:** If the analysis results are positive to potential evidence admissible to the ICC, the accredited entity will treat it as such and ensure the record is ready to be submitted to the MTB for Prosecution's assessment. The evidence is also 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.
4. **Creates records in MTB:** as soon as the data is 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.
5. **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:** Should the outcomes of the evidence review be unsatisfactory, a new block in the MTB will be created to update this updated status.

b. **Informs accredited entity of its inadmissibility:** The prosecution team informs the accredited entity with the conclusions of its review.

6. **Creates record in MTB:** This activity derives from direct action from the Prosecution Team, which has acquired evidence and creates the record immediately, without third party review.
7. **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.



Evidence acquisition
Evidence review
Evidence acquisition and review
Non-accredited entity
Accredited entity
Prosecution team
MultiTrustBloc
Captures possible
Submits data to accredited entity
Validates suitability of data
Is it possible
No
Yes
Informs local citizen/entity of its inadmissabili
Data retained in local storage
Captures possible
Treats data as evidence and creates a snapshot
Creates record in MTB
Notifies Prosecution team of addition
Reviews evidence
Is it suitable for the case?
No
Updates record in MTB setting status as
Informs accredited entity of its inadmissibility
Record reviewed and considered inadmissible
Creates new block with updated Status
Captures evidence
Creates record in MTB
Updates record in MTB and retrieves evidence to its
Record accepted as evidence
First Block
First Block
Evidence retrieved
Creates new block
Creates new block with updated Status

Figure 7 - Evidence acquisition process

Evidence usage and disclosure process

Once the data is analysed and considered as evidence, it resides under the Prosecution team's custody until it is required to be used for review and to build the case against a suspect. This process starts when there is the need to evaluate specific evidence and is depicted in Figure 8.

1. **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 action.
2. **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.
3. **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.
4. **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 Defence or Victims representatives’ teams.
5. **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 Judges Chamber is notified of evidence transfer and custody in their control.
   c. **Receives notification of access to the record:** Involved parties are notified that new evidence is available for their review.
6. **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.

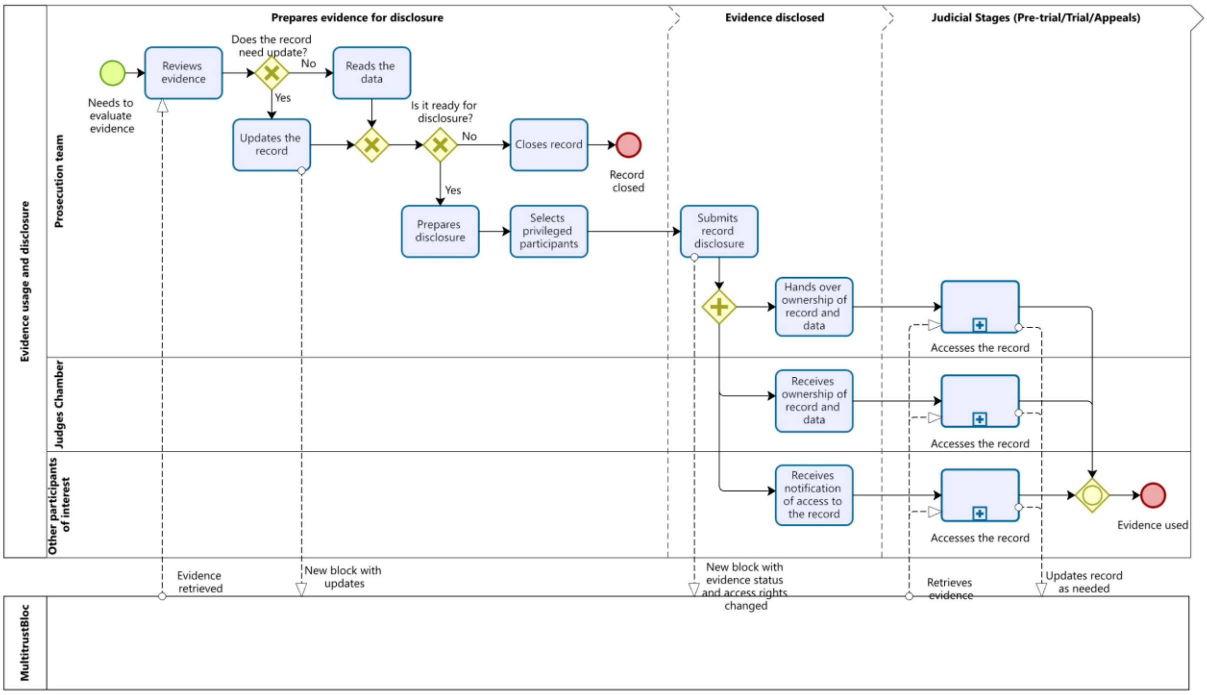

Evidence usage and disclosure
Prosecution team
Judges Chamber
Other participants of interest
MultitrustBloc
Prepares evidence for disclosure
Evidence disclosed
Judicial Stages (Pre-trial/Trial/Appeals)
Needs to evaluate evidence
Reviews evidence
Does the record need update?
No
Yes
Reads the data
Updates the record
Is it ready for disclosure?
No
Yes
Closes record
Record closed
Prepares disclosure
Selects privileged participants
Submits record disclosure
Hands over ownership of record and data
Receives ownership of record and data
Receives notification of access to the record
Accesses the record
Accesses the record
Accesses the record
Evidence used
Evidence retrieved
New block with updates
New block with evidence status and access rights changed
Retrieves evidence
Updates record as needed

Figure 8 – Evidence usage and disclosure process

4.4. Solution Design

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 ICC's jurisdiction that is decentralized, 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 thorough evaluation. The ICC could also have the role of Accredited Organization, allowing a direct contact with people and evaluation of submissions from the source.

Once the accredited entity receives the evidence candidate and considers it suitable for the Prosecution team's review, it creates a new record in the MTB to store a baseline of the possible evidence.

Evidence can be of digital or physical nature, and for each a different storage repository will be required, a virtual vault for the former and a physical vault for the latter. When the accredited entity validates the submission, it is moved to the respective repository, which the prosecution team has access to, for when it will need to evaluate the evidence.

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 Prosecution, Judiciary and other interested parties to make it robust, credible and tamper-proof.

Figure 9 provides a high-level view of how the system will interact with evidence and its multiple parties.

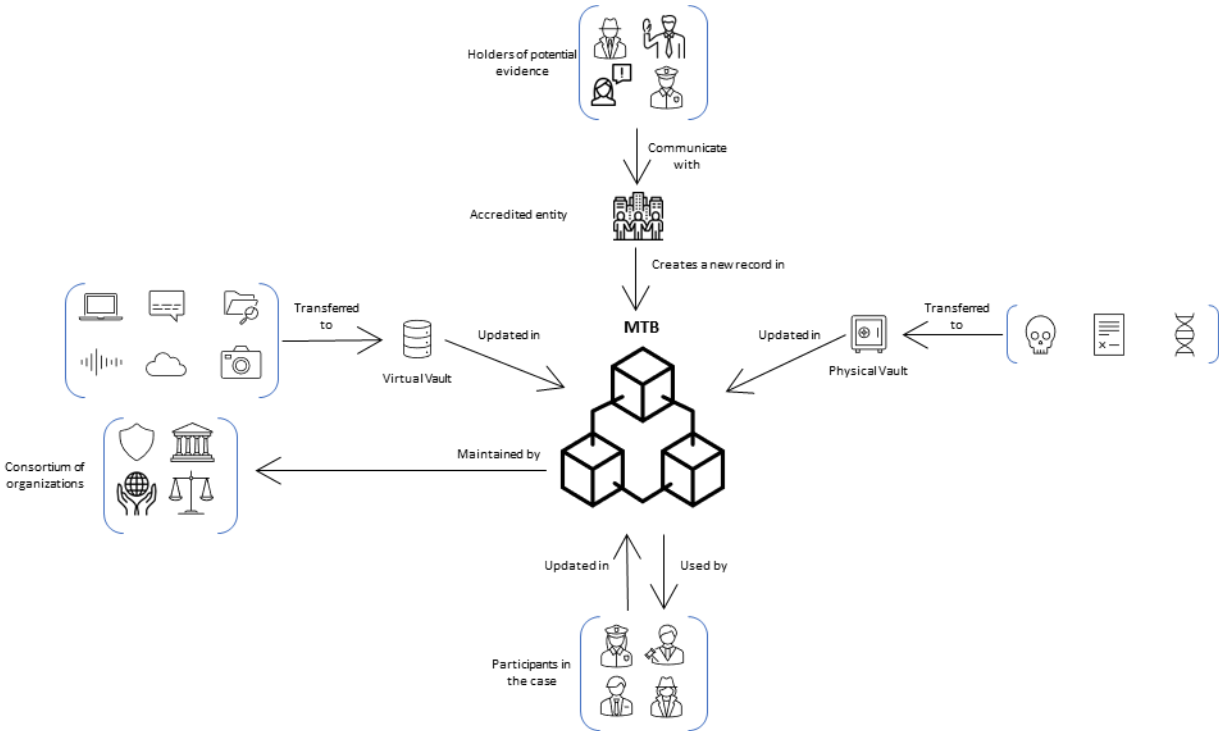


Figure 9 - High level view of MultiTrustBloc

Governance Model

Roles and Responsibilities

The MTB is supported by two groups of entities that bring different roles to the solution. The first and critical group consists of primary entities, represented by the Court 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 second is the secondary entities group, which consists of any accredited entity by the primary entities that wishes to participate in the advancement of justice, by helping to maintain the blockchain and validate new blocks within it.

Consensus Mechanism

Given the Consortium characteristics of this blockchain, the consensus mechanism selected was Practical Byzantine Fault Tolerance [53], due to its performance in validating transactions and 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. Small version changes require only agreement from the two primary entities, while a major change would require both primary entities to agree plus a majority of secondary entities.

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. All members can also propose and add new blocks in the blockchain.

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 Prosecution and the Court Chambers, elected representatives from the ASP will decide on how to settle the dispute.

Upgrades and Forks

Protocol upgrades to the MTB are proposed jointly by 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, mandated by the ASP to guarantee the integrity of the blockchain and smart contracts.

Evidence Records State lifecycle.

As the judicial process progresses, from non-existent to appeals and reparations, the evidence progresses into different states, according to its validity as evidence within a specific case. Below are represented the major lifecycle states that evidence could have.

1. Pre-Artifact creation: Before an artifact is formally recognized and documented within the ICC's system, the potential evidence or information resides externally. This could be information or potential evidence that has been identified by external entities, witnesses, or other sources but has not yet been introduced or documented within the ICC's formal evidence management system. It represents raw, unprocessed data or information that may hold potential evidentiary value.
2. Artifact created: This is the inception point where a piece of evidence or an artifact is first identified and documented as such. It signifies the initial recognition of potential evidence.
3. Submitted for prosecution review: The artifact, once created, is presented for preliminary assessment by the prosecution team to determine its relevance and potential significance to the case.
4. Pending review: At this juncture, 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 custody: The approved evidence is now formally in the custody of the prosecution, 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, either for potential appeals or as a record.
14. Archived (from retained): After the retention period, the evidence is moved to long-term storage, ensuring it remains accessible for any future legal or academic 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 10 depicts all the lifecycle stages an artifact can have in the MTB.

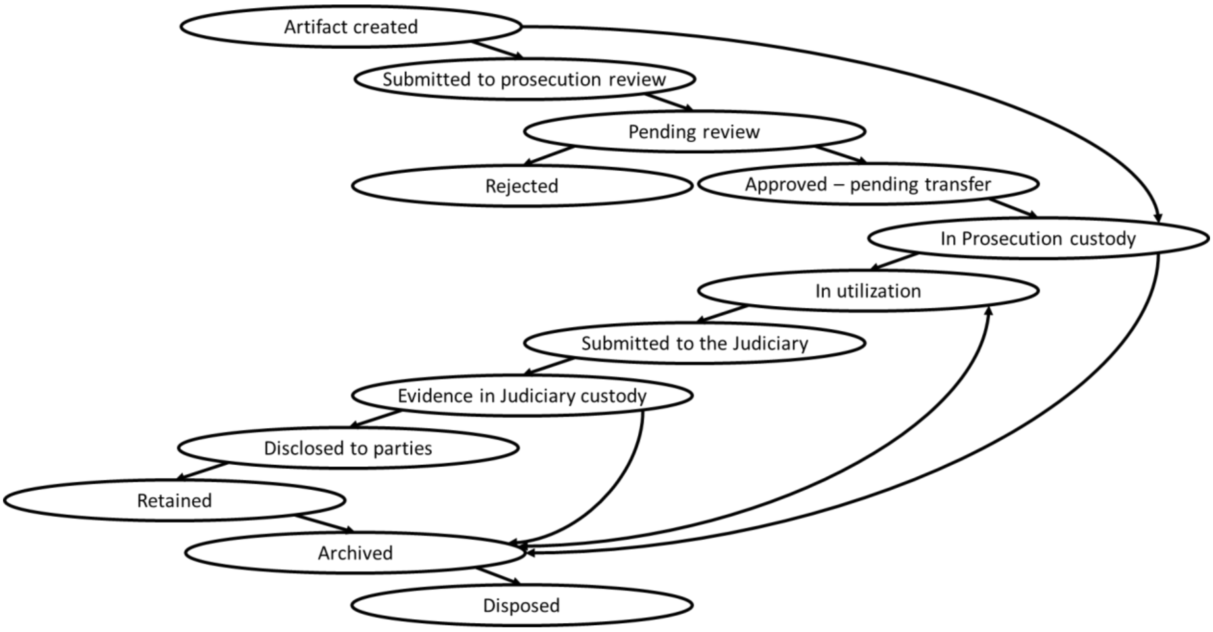


Figure 10 - Evidence Lifecycle stages

4.5. Application mock-ups

To provide a more tangible and visual depiction of the solution, a set of mock-ups was created. These mock-ups are a representation of the solution as viewed by the different participants and had as focus the feasibility of implementation of the solution through a web page.

In order to ensure an objective approach to the creation of the user interfaces relevant to the MultiTrustBloc, the content of these webpages was created based on the needs of the process step they are relevant in, and also inspired in ICC's website called OTP Link which serves the purpose of submitting online evidence directly to the Prosecution of this institution [54]. Considering the user interface (UI) and experience (UX) for the website mock-ups, it was relevant to consider a framework that would provide a set of features that could guide its build up.

Zhang et al [55] provide a model for website design based on two factors: hygiene and motivator. The first focuses on factors addressing functionality and serviceability, while the second on factors which contribute to user satisfaction. The framework being presented in this dissertation is conceptualized to be the place where evidence is submitted with regards to crimes within the ICC's jurisdiction and being such a novel proposal within the international criminal justice, the focus of these mock-ups was based on hygiene factors, leaving the motivator factors for a further iteration of this framework.

From their work, a total of six categories is identified as being part of the hygiene factors group, presented below and in order of descending percentage frequency difference:

1. Category 07: Technical aspects
2. Category 08: Navigation
3. Category 04: Privacy and Security
4. Category 01: Surfing Activity
5. Category 11: Impartiality
6. Category 12: Information Content

Each category consists of a set of features that were evaluated and eight were selected as being the most relevant for this type of solution, presented in Table 4.

Table 4 - Website feature evaluation guidelines

Category ID	Feature	Feature requirement justification
12-8	Content that supports/does not support the Website's intended purpose	It is critical for the website to provide the people submitting, reviewing and disclosing the evidence, as many capabilities as possible to allow them to discharge their actions. All information required in the processes should be clearly requested.
8-3	Clear/unclear directions for navigating the Website	Each stage of the process should be well defined to avoid misunderstandings and input of data in incorrect location.
8-1	Presence/absence of indicators of the user's location within the Website	In the case of MTB, it is important for the user to know which IP they are displaying to it, so they can understand the risks of personal harm if contact is made from that internet location to the solution.
12-3	Accurate/inaccurate information.	All information available and input fields should be clearly and factually identified.
8-2	Effective/ineffective navigation aids.	Navigation should be clear and associated with the stage of the process of the action being taken.
4-3	Authorized/unauthorized collection of user data.	Collection of user data should only take place if approved by the user, and clearly stated when that is being happening.
9-2	Structure of information presentation is logical/illogical.	Information presented and requested should have an easy-to-understand structure and information clearly visible.
4-1	Presence/absence of access requirement.	For submission of evidence the access should be made open to the public, but all subsequent activities should be taken by authenticated users.

Submission of evidence

Figure 11 represents the webpage allowing any user to submit evidence that they consider to be within the jurisdiction of the ICC, and there they would be able to add the evidence and relevant metadata such as description of the incident, place, and data where it took place. They would also be able to select an accredited entity they trust to do a preliminary review of the submission. There is also the possibility of making this submission anonymous, should there be any concerns on personal injury from the person submitting it.

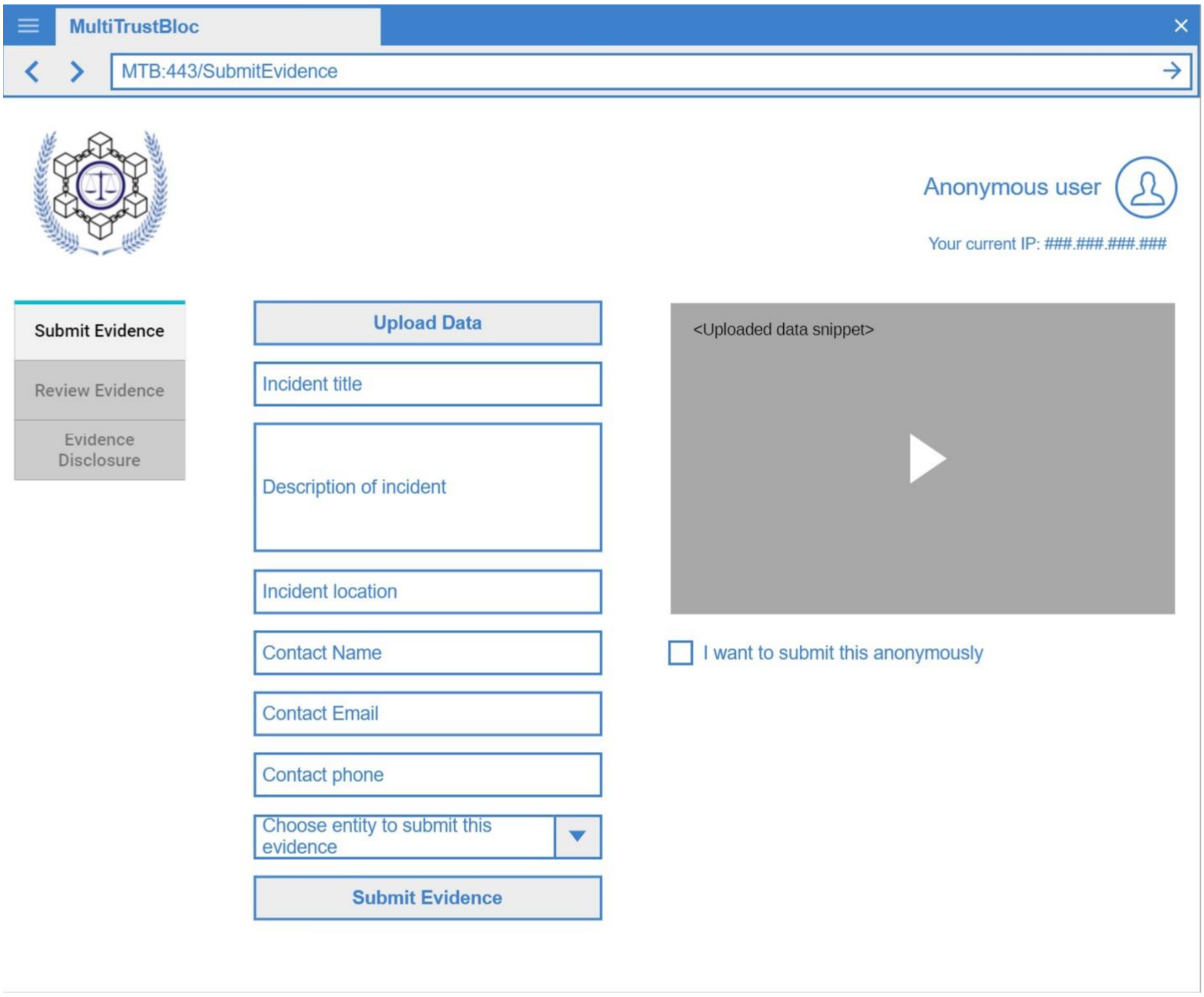
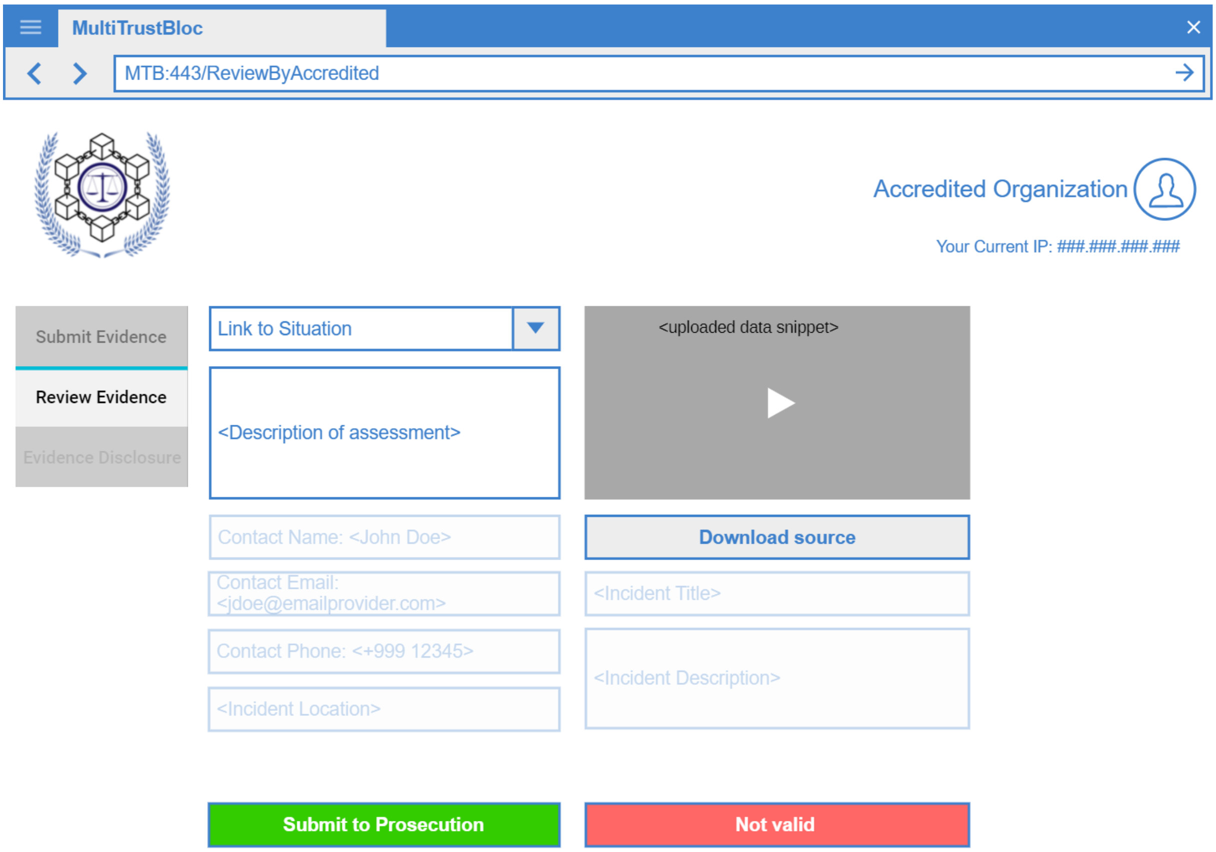


Figure 11 - Submit evidence mock-up.

Accredited entity review

Figure 12 presents the view of an accredited organization reviewing a submission from a user not known to the ICC. The reviewer evaluates the merit of the submission and decides if this is a valid or invalid submission. Before this decision, there is the possibility of downloading the data source, and link to a situation, for easier assessment from the respective team, including an assessment and description of the review for more context on the decision from this reviewer.



MTB:443/ReviewByAccredited

Accredited Organization

Your Current IP: ###.###.###.###

Link to Situation

<Description of assessment>

<uploaded data snippet>

Contact Name: <John Doe>

Contact Email: <jdoe@emailprovider.com>

Contact Phone: <+999 12345>

<Incident Location>

<Incident Title>

<Incident Description>

Figure 12 - Accredited entity review

First prosecution review

Figure 13 displays the first time a member of the prosecution team assigned to this case reviews the evidence, being able to see the evidence and related metadata, as well as incorporate any comments they consider relevant to the case or to contextualize the data. Once it is reviewed and evaluated, the prosecution team will deliberate if this piece of information is to be moved forward to the case as possible evidence or rejected as such.

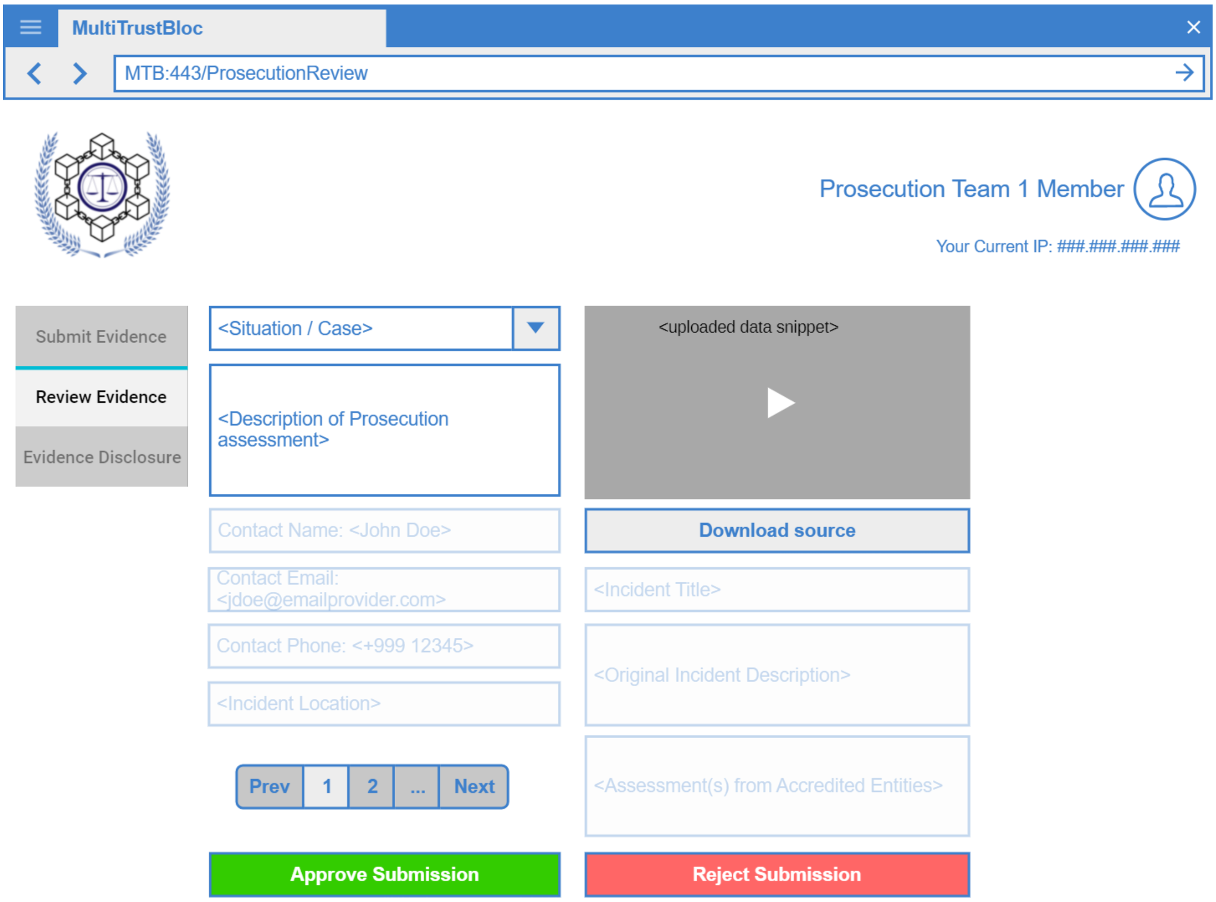

MultiTrustBloc
MTB:443/ProsecutionReview
Prosecution Team 1 Member
Your Current IP: ###.###.###.###
Submit Evidence
Review Evidence
Evidence Disclosure
<Situation / Case>
<Description of Prosecution assessment>
Contact Name: <John Doe>
Contact Email: <jdoe@emailprovider.com>
Contact Phone: <+999 12345>
<Incident Location>
Prev
1
2
...
Next
Approve Submission
<uploaded data snippet>
Download source
<Incident Title>
<Original Incident Description>
<Assessment(s) from Accredited Entities>
Reject Submission

Figure 13 – First prosecution review

Subsequent prosecution review(s)

Figure 14 represents the view of a piece of evidence that is being updated with more information or analysis from the prosecution team. This could be the linking of another evidence to this, or reference to other possible event where this evidence might be related to.

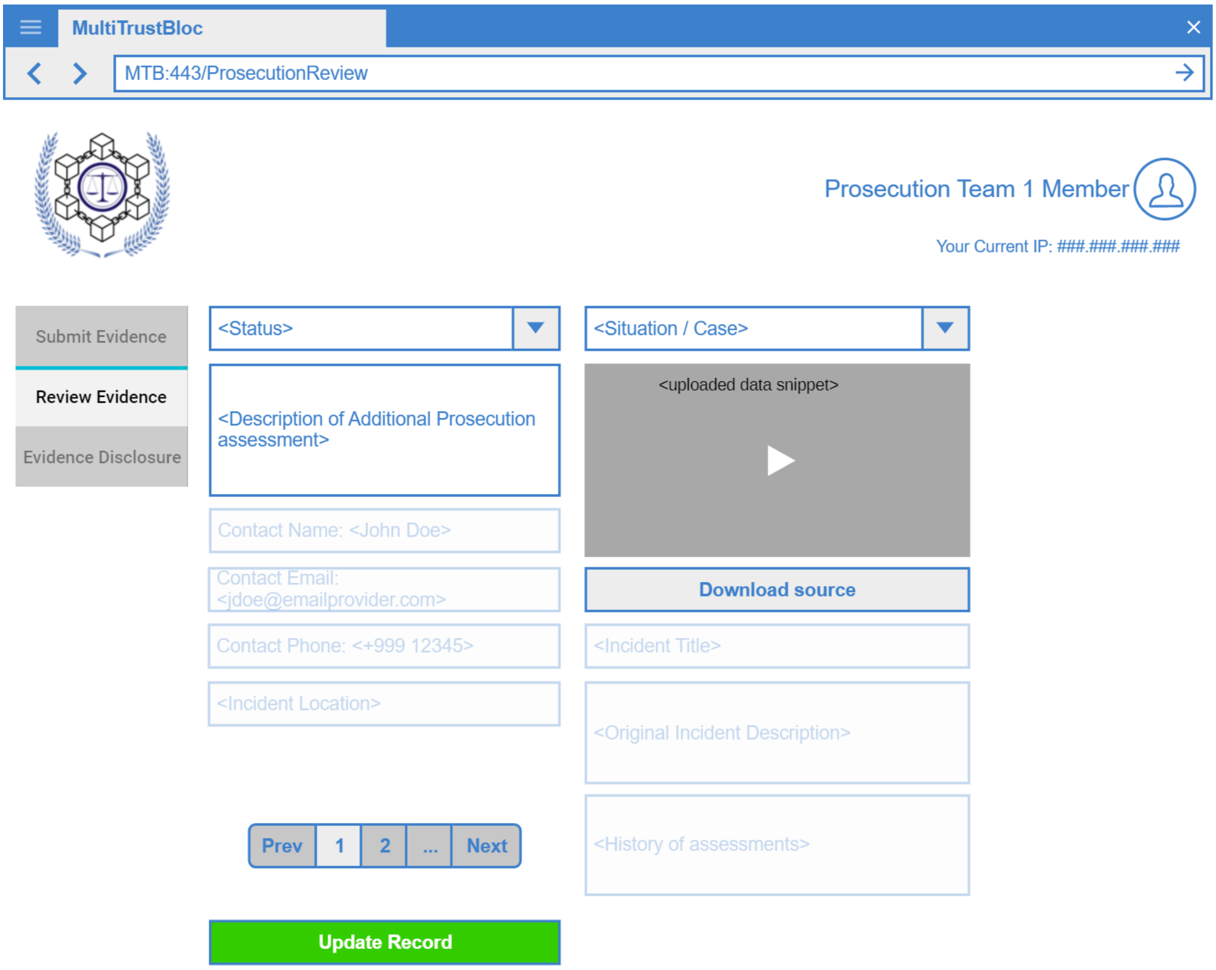
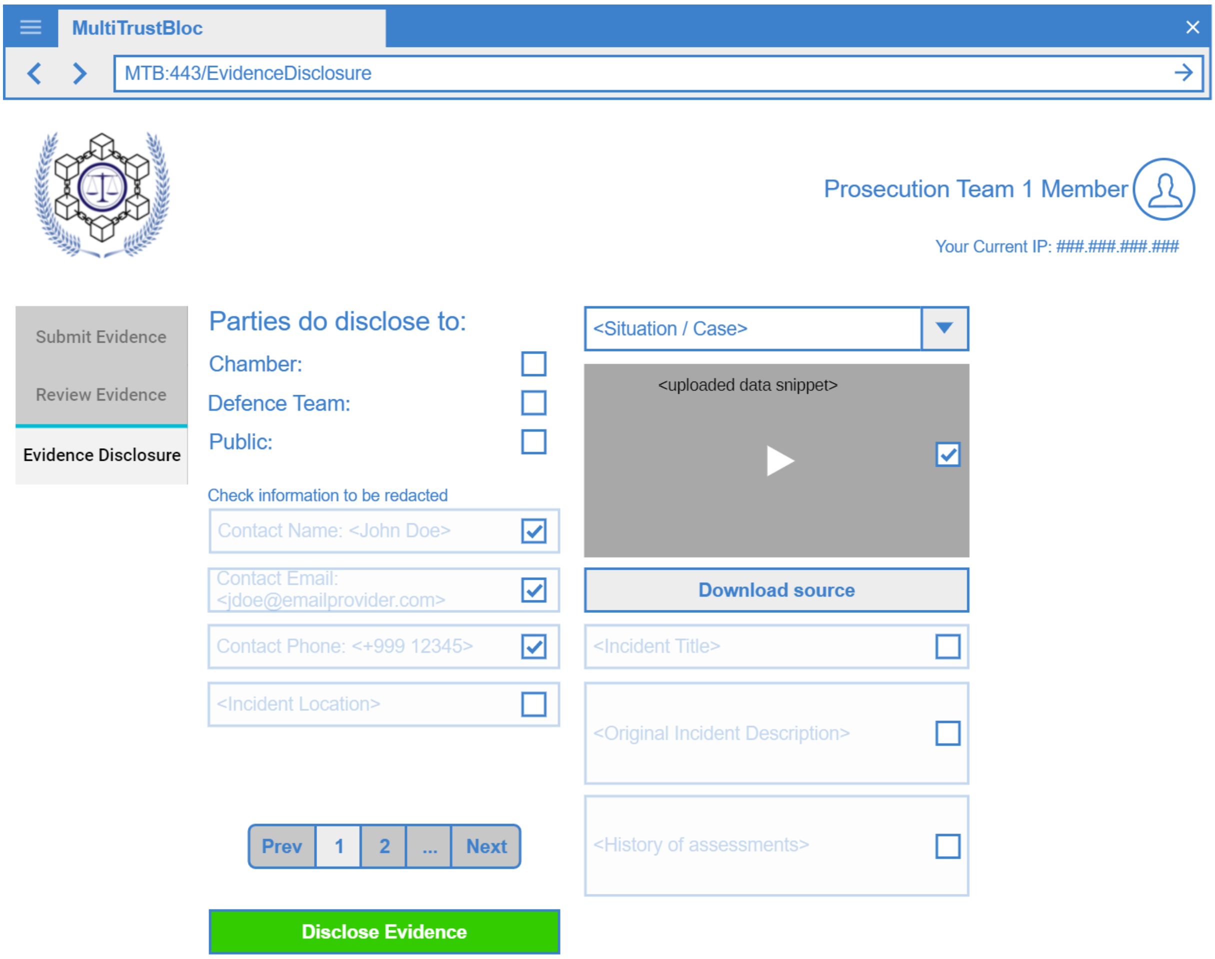


Figure 14 – Subsequent prosecution review(s)

Evidence disclosure

Figure 15 displays the last moment before the evidence is disclosed to other parties than the prosecution. The user is able to select to which parties the evidence should be disclosed to, including if this is a public disclosure or not.



Parties do disclose to:

Chamber: □

Defence Team: □

Public: □

Check information to be redacted

Contact Name: <John Doe> ☑

Contact Email: <jdoe@emailprovider.com> ☑

Contact Phone: <+999 12345> ☑

<Incident Location> □

<Situation / Case>

<uploaded data snippet> ☑

<Incident Title> □

<Original Incident Description> □

<History of assessments> □

Figure 15 – Evidence disclosure

4.6. Artifact evaluation

The MultiTrustBloc framework was presented individually to each of the three panel members introduced in section 1.4 Methodology during the month of November. 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 shared for the evaluation of each participant. The survey questions consisted of the objective statements presented previously in Table 1, instantiated from the DSR Evaluation Framework. Table 5 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, and 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 5 - 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

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 of the same questions as the ones answered by the panel, and had supporting material explaining the MultiTrustBloc framework and had 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 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% Male and an average age of 44,7 years. The median of the participants was 43 years. The standard deviation 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 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 include**d** 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. 53% of the respondents had a managerial role.

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

For the purpose of this dissertation, 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 have most have specialism 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, en-suring the organization has the right technological tools and maintain them in good order to support the judicial process. The focus of this group is in technological aspects and the understanding on legal affairs within the context of the mandate of the organization is superficial is most situations. 10 individuals (59%) within this category responded to the survey.

The results discussed consider the two categories combined.

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 MultiTrustBloc framework would meet the artifact evaluation objectives set.

Table 6 presents the average results from the extended user evaluation survey.

Table 6 - 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 16 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.

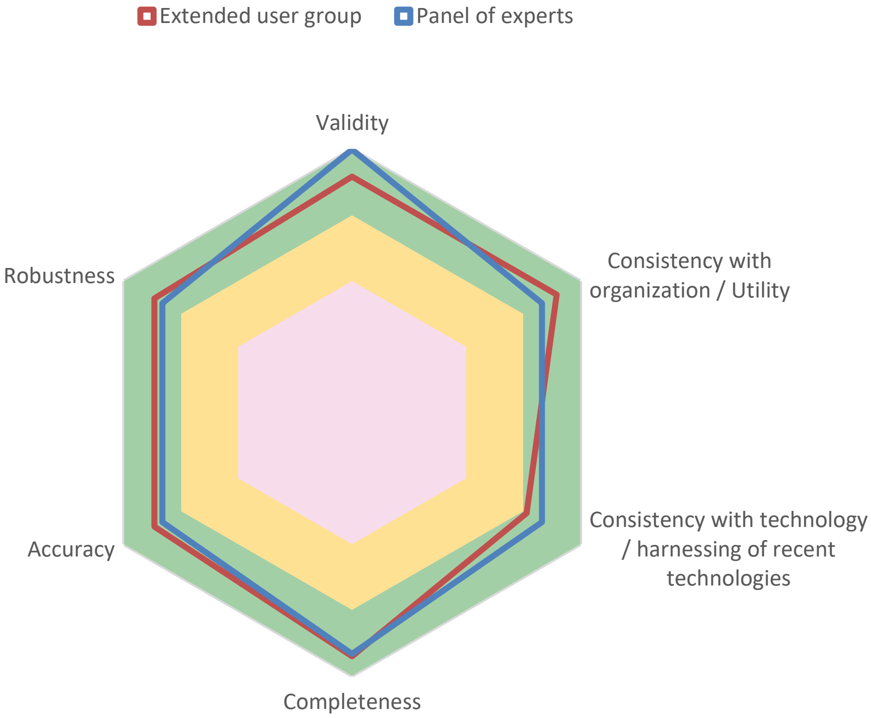


Figure 16 - Evaluation comparison per criteria

CHAPTER 5

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 International Criminal Court, it is to bring an end to impunity, and justice and reparations to its victims.

The DSRM approach was adopted, and as such, the six stages of this approach were considered, which were divided within this dissertation in four major work packages.

The first stage – Problem identification and motivation; was fulfilled with the identification of the added value of blockchain technology within the area of evidence management and chain of custody within the sector. This was evaluated and validated using the Blue Ocean Strategy methodology.

The second stage – solution objectives; of the solution was enabled and enriched with the literature review, which provided valuable insights of what was found in the body of knowledge.

The third and fourth stages – design, development, and demonstration; are covered and depicted in the MultiTrustBloc framework.

The fifth stage – evaluation; leveraged a panel of experts in this area within the sector of international criminal justice, providing a validation of the usefulness of such solution.

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

5.1. 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.

Related work

The related work 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 even more novel. Using the PRISMA methodology and focusing on five key attributes of this dissertation, it was clear that while some papers covered some areas, no paper within academic literature covered the five key attributes considered here: 1) Blockchain, 2) Chain of Custody, 3) Evidence management, 4) Multi-level trust and 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 Framework

This dissertation concludes with the MultiTrustBloc framework, which provides a design for a blockchain based system that would enable the International Criminal Court 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 define. 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 MultiTrustBloc 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 International Criminal Court.

5.2. Communication

This dissertation contributed to the scientific community in several aspects, which are detailed in this section.

Engaged with experts in the field of International Criminal Justice, particularly in the evidence management and technology areas.

Discussed with IT management in the field of International Criminal Justice the benefits of blockchain technology in evidence management and chain of custody.

This dissertation served as basis for two publications approved and presented at IBICA 2023 Conference [56] with the following titles:

- Barranha Rodrigues dos Santos, Nuno M; Curado Silveirinha, Joel; Ferreira, João Carlos A "Blockchain's Potential in International Criminal Justice: A Blue Ocean Analysis and Literature Review"
- Barranha Rodrigues dos Santos, Nuno M; Ferreira, João Carlos A; Curado Silveirinha, Joel. "Multiparty Trust Levels in Evidence Management: Ensuring Tamper-Proof Chain of Custody in Blockchain"

This work is accepted for publication in Springer book chapter of *Lecture Notes in Networks and Systems*

5.3. Future work

This dissertation 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, them being:

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

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

2. Study for a mobile phone-based application that guarantees authenticity from data capture 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 court.

3. Study the use of motivating factors in the creation of the MultiTrustBloc 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 MultiTrustBloc.

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.

Bibliographic References

[1] O. Mosweu and T. Mosweu, “The Influence of Archives in Conflict Resolution: A Case Study of Botswana and Namibia,” *Afr. J. Libr. Arch. Inf. Sci.*, vol. 33, no. 1, pp. 23–36, 2023.

[3] J. K. Cogan, “The Problem of Obtaining Evidence for International Criminal Courts,” *Hum. Rights Q.*, vol. 22, no. 2, pp. 404–427, 2000, doi: 10.1353/hrq.2000.0021.

[4] *Rome Statute of the International Criminal Court*. The Netherlands: International Criminal Court, 2011. Accessed: Jun. 09, 2023. [Online]. Available: https://www.icc-cpi.int/sites/default/files/RS-Eng.pdf

[5] *Rules of Procedure and Evidence*, Second. The Netherlands: International Criminal Court, 2013. Accessed: Jun. 09, 2023. [Online]. Available: https://www.icc-cpi.int/sites/default/files/RulesProcedureEvidenceEng.pdf

[6] “About the Court,” International Criminal Court. Accessed: Sep. 10, 2023. [Online]. Available: https://www.icc-cpi.int/about/the-court

[7] Public Information and Outreach Section, *understanding-the-icc.pdf*. Oude Waalsdorperweg 10, 2597 AK, The Hague, The Netherlands. Accessed: Sep. 10, 2023. [Online]. Available: https://www.icc-cpi.int/sites/default/files/Publications/understanding-the-icc.pdf

[8] B. R. Ulbricht, C. Moxley, M. D. Austin, and M. D. Norburg, “Digital Eyewitnesses: Using New Technologies to Authenticate Evidence in Human Rights Litigation,” 2022.

[9] P. A. Bernstein and N. Goodman, “Concurrency Control in Distributed Database Systems,” *ACM Comput. Surv. CSUR*, vol. 13, no. 2, pp. 185–221, 1981, doi: 10.1145/356842.356846.

[10] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, Accessed: Jun. 09, 2023. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[11] V. Ali, A. A. Norman, and S. R. B. Azzuhri, “Characteristics of Blockchain and Its Relationship With Trust,” *IEEE Access*, vol. 11, pp. 15364–15374, 2023, doi: 10.1109/ACCESS.2023.3243700.

[12] S. Meunier, “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*, 2018, pp. 23–34. doi: 10.1016/B978-0-12-814447-3.00003-3.

[13] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, “A Design Science Research Methodology for Information Systems Research,” *J. Manag. Inf. Syst.*, vol. 24, no. 3, pp. 45–77, Dec. 2007, doi: 10.2753/MIS0742-1222240302.

[14] A. R. Hevner, S. T. March, J. Park, and S. Ram, “Design Science in Information Systems Research,” *MIS Q.*, vol. 28, no. 1, pp. 75–105, 2004, doi: 10.2307/25148625.

[15] N. Prat, I. Comyn-Wattiau, and J. Akoka, “Artifact evaluation in Information Systems design-science research - A holistic view,” *PACIS 2014 Proc.*, Jan. 2014, [Online]. Available: https://aisel.aisnet.org/pacis2014/23

[16] A. Joshi, S. Kale, S. Chandel, and D. Pal, “Likert Scale: Explored and Explained,” *Br. J. Appl. Sci. Technol.*, vol. 7, pp. 396–403, Jan. 2015, doi: 10.9734/BJAST/2015/14975.

[17] M. J. Page, J. E. McKenzie, P. M. Bossuyt, I. Boutron, T. C. Hoffmann, C. D. Mulrow, L. Shamseer, J. M. Tetzlaff, E. A. Akl, S. E. Brennan, R. Chou, J. Glanville, J. M. Grimshaw, A. Hróbjartsson, M. M. Lalu, T. Li, E. W. Loder, E. Mayo-Wilson, S. McDonald, L. A. McGuinness, L. A. Stewart, J. Thomas, A. C. Tricco, V. A. Welch, P. Whiting, and D. Moher, “The PRISMA 2020 statement: an updated guideline for reporting systematic reviews,” *BMJ*, p. n71, Mar. 2021, doi: 10.1136/bmj.n71.

[18] W. C. Kim and R. Mauborgne, “Blue Ocean Strategy,” *Harvard Business Review*, Oct. 01, 2004. Accessed: Jun. 15, 2023. [Online]. Available: https://hbr.org/2004/10/blue-ocean-strategy

[19] F. Awladthani, S. Porkodi, R. Saranya, and V. Pandurengan, “A systematic literature review of the adoption of a blue ocean strategy by small and medium enterprises for sustainable growth,” *J. Sustain. Sci. Manag.*, vol. 18, pp. 197–230, Feb. 2023, doi: 10.46754/jssm.2023.02.014.

[20] P. Jindal and L. Chavan, “Role of Blockchain Technology in Creating Blue Ocean Strategy for Banking Products and Services,” in *Contemporary Studies of Risks in Emerging Technology, Part B*, S. Grima, K. Sood, and E. Özen, Eds., in Emerald Studies in Finance, Insurance, and Risk Management. , Emerald Publishing Limited, 2023, pp. 169–182. doi: 10.1108/978-1-80455-566-820231008.

[21] A. Y. Nasereddin, “Impact of the Blue Ocean Strategy Dimensions in Achieving Competitive Advantage from the Perspective of Faculty Members,” *Inf. Sci. Lett.*, vol. 12, no. 6, pp. 2685–2698, Jun. 2023, doi: 10.18576/isl/120639.

[22] C. Kim, K. H. Yang, and J. Kim, “A strategy for third-party logistics systems: A case analysis using the blue ocean strategy,” *Omega*, vol. 36, no. 4, pp. 522–534, Aug. 2008, doi: 10.1016/j.omega.2006.11.011.

[23] A. J. Ehrenberg and J. L. King, “Blockchain in Context,” *Inf. Syst. Front.*, vol. 22, no. 1, pp. 29–35, 2020, doi: 10.1007/s10796-019-09946-6.

[24] O. Olukoya, “Distilling blockchain requirements for digital investigation platforms,” *J. Inf. Secur. Appl.*, vol. 62, 2021, doi: 10.1016/j.jisa.2021.102969.

[25] A. A. Khan, M. Uddin, A. A. Shaikh, A. A. Laghari, and A. E. Rajput, “MF-Ledger: Blockchain Hyperledger Sawtooth-Enabled Novel and Secure Multimedia Chain of Custody Forensic Investigation Architecture,” *IEEE Access*, vol. 9, pp. 103637–103650, 2021, doi: 10.1109/ACCESS.2021.3099037.

[26] D. Jaquet-Chiffelle, E. Casey, and J. Bourquenoud, “Tamperproof timestamped provenance ledger using blockchain technology,” *FORENSIC Sci. Int.-Digit. Investig.*, vol. 33, Jun. 2020, doi: 10.1016/j.fsidi.2020.300977.

[27] G. Liu, J. He, and X. Xuan, “A Data Preservation Method Based on Blockchain and Multidimensional Hash for Digital Forensics,” *Complexity*, vol. 2021, 2021, doi: 10.1155/2021/5536326.

[28] M. Ali, A. Ismail, H. Elgohary, S. Darwish, and S. Mesbah, “A Procedure for Tracing Chain of Custody in Digital Image Forensics: A Paradigm Based on Grey Hash and Blockchain,” *Symmetry*, vol. 14, no. 2, 2022, doi: 10.3390/sym14020334.

[29] R. Sathyaprakasan, P. Govindan, S. Alvi, L. Sadath, S. Philip, and N. Singh, “An Implementation of Blockchain Technology in Forensic Evidence Management,” in *Proc. IEEE Int. Conf. Comput. Intell. Knowl. Econ., ICCIKE*, Naranje V., Singh B., and Velan S., Eds., Institute of Electrical and Electronics Engineers Inc., 2021, pp. 208–212. doi: 10.1109/ICCIKE51210.2021.9410791.

[30] X. Burri, E. Casey, T. Bollé, and D.-O. Jaquet-Chiffelle, “Chronological independently verifiable electronic chain of custody ledger using blockchain technology,” *Forensic Sci. Int. Digit. Investig.*, vol. 33, 2020, doi: 10.1016/j.fsidi.2020.300976.

[31] F. E. Alruwaili, “CustodyBlock: A Distributed Chain of Custody Evidence Framework,” *Information*, vol. 12, no. 2, p. 88, Feb. 2021, doi: 10.3390/info12020088.

[32] R. S. Kusuma, “Digital Evidence Security System Design Using Blockchain Technology,” *Int. J. Saf. Secur. Eng.*, vol. 13, no. 1, pp. 159–165, 2023, doi: 10.18280/ijsse.130118.

[33] S. H. Gopalan, S. A. Suba, C. Ashmithashree, A. Gayathri, and V. Jebin Andrews, “Digital forensics using blockchain,” *Int. J. Recent Technol. Eng.*, vol. 8, no. 2 Special Issue 11, pp. 182–184, 2019, doi: 10.35940/ijrte.B1030.0982S1119.

[34] Y. Zhang, S. Wu, B. Jin, and J. Du, “A blockchain-based process provenance for cloud forensics,” in *IEEE Int. Conf. Comput. Commun., ICCC*, Institute of Electrical and Electronics Engineers Inc., 2018, pp. 2470–2473. doi: 10.1109/CompComm.2017.8322979.

[35] B. M. Manjre and K. K. Goyal, “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., 2023. doi: 10.1063/5.0127910.

[36] S. Bonomi, M. Casini, and C. Ciccotelli, “B-CoC: A blockchain-based chain of custody for evidences management in digital forensics,” in *OpenAccess Ser. Informatics*, Danos V., Herlihy M., Potop-Butucaru M., Prat J., and Tucci-Piergiovanni S., Eds., Schloss Dagstuhl-Leibniz-Zentrum fur Informatik GmbH, Dagstuhl Publishing, 2020. doi: 10.4230/OASIcs.Tokenomics.2019.12.

[37] W. Yan, J. Shen, Z. Cao, and X. Dong, “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, May 2020, pp. 19–23. doi: 10.1145/3390566.3391690.

[38] D. Boneh, B. Lynn, and H. Shacham, “Short Signatures from the Weil Pairing,” *J. Cryptol.*, vol. 17, no. 4, pp. 297–319, Sep. 2004, doi: 10.1007/s00145-004-0314-9.

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

[40] M. Chopade, S. Khan, U. Shaikh, and R. Pawar, “Digital Forensics: Maintaining Chain of Custody Using Blockchain,” in *Proc. Int. Conf. I-SMAC IoT Soc., Mob., Anal. Cloud, I-SMAC*, Institute of Electrical and Electronics Engineers Inc., 2019, pp. 744–747. doi: 10.1109/I-SMAC47947.2019.9032693.

[41] A. H. Lone and R. N. Mir, “Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer,” *Digit. Investig.*, vol. 28, pp. 44–55, Mar. 2019, doi: 10.1016/j.diin.2019.01.002.

[42] U. Feige, A. Fiat, and A. Shamir, “Zero-knowledge proofs of identity,” *J. Cryptol.*, vol. 1, no. 2, pp. 77–94, 1988, doi: 10.1007/BF02351717.

[43] K. Awuson-David, T. Al-Hadhrami, M. Alazab, N. Shah, and A. Shalaginov, “BCFL logging: An approach to acquire and preserve admissible digital forensics evidence in cloud ecosystem,” *Future Gener. Comput. Syst.*, vol. 122, pp. 1–13, 2021, doi: 10.1016/j.future.2021.03.001.

[44] H. Al-Khateeb, G. Epiphaniou, and H. Daly, “Blockchain for modern digital forensics: The chain-of-custody as a distributed ledger,” in *Adv. Sci. Tech. Sec. Appl.*, Springer, 2019, pp. 149–168. doi: 10.1007/978-3-030-11289-9_7.

[45] M. Li, C. Lal, M. Conti, and D. Hu, “LEChain: A blockchain-based lawful evidence management scheme for digital forensics,” *Future Gener. Comput. Syst.- Int. J. Escience*, vol. 115, pp. 406–420, Feb. 2021, doi: 10.1016/j.future.2020.09.038.

[46] A. Shahaab, C. Hewage, and I. Khan, “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, Jul. 2021, pp. 45–52. doi: 10.1145/3460537.3460550.

[47] F.-C. Tsai, “The Application of Blockchain of Custody in Criminal Investigation Process,” in *Knowledge-Based and Intelligent Information & Engineering Systems (kse 2021)*, J. Watrobski, W. Salabun, C. Toro, C. Zanni-Merk, R. J. Howlett, and L. C. Jain, Eds., Amsterdam: Elsevier Science Bv, 2021, pp. 2779–2788. doi: 10.1016/j.procs.2021.09.048.

[48] “Home | ethereum.org.” Accessed: Jul. 18, 2023. [Online]. Available: https://ethereum.org/en/

[49] P. Sanda, D. Pawar, and V. Radha, “Blockchain-based tamper-proof and transparent investigation model for cloud VMs,” *J. Supercomput.*, vol. 78, no. 16, pp. 17891–17919, Nov. 2022, doi: 10.1007/s11227-022-04567-4.

[50] T. Martin and M. Hammoudeh, “Data Preservation System using BoCA: Blockchain-of-Custody Application,” in *The 5th International Conference on Future Networks & Distributed Systems*, in ICFNDS 2021. New York, NY, USA: Association for Computing Machinery, Apr. 2022, pp. 70–77. doi: 10.1145/3508072.3508084.

[51] P. Akello, N. Vemprala, N. Lang Beebe, and K.-K. Raymond Choo, “Blockchain Use Case in Ballistics and Crime Gun Tracing and Intelligence: Toward Overcoming Gun Violence,” *ACM Trans. Manag. Inf. Syst.*, vol. 14, no. 1, p. 7:1-7:26, Feb. 2023, doi: 10.1145/3571290.

[52] “BPMN Specification - Business Process Model and Notation.” Accessed: May 02, 2023. [Online]. Available: https://www.bpmn.org/

[53] M. Castro and B. Liskov, “Practical Byzantine Fault Tolerance”.

[54] “OTP Link.” Accessed: Nov. 19, 2023. [Online]. Available: https://otplink.icc-cpi.int/

[55] P. Zhang and G. M. Von Dran, “Satisfiers and dissatisfiers: a two-factor model for website design and evaluation,” *J. Am. Soc. Inf. Sci. Technol.*, vol. 51, no. 14, pp. 1253–1268, 2000, doi: 10.1002/1097-4571(2000)9999:9999<::AID-ASI1039>3.0.CO;2-O.

[56] “IBICA 2023 (December 14-15, 2023 in On the World Wide Web).” Accessed: Dec. 09, 2023. [Online]. Available: https://www.mirlabs.org/ibica23/