Blockchain Based Criminal Records Management System in Sri Lanka

Project ID – 2023-270

M.Thushitharan

(IT19983370)

Bachelor of Science (Hons) in Information Technology

Specializing in Cyber Security

Department of Computer System and Engineering

Sri Lanka Institute of Information Technology

September 2023

Blockchain Based Criminal Records Management System in Sri Lanka

Project ID – 2023-270

Thushitharan M.

(IT19983370)

Bachelor of Science (Hons) in Information Technology

Specializing in Cyber Security

Department of Computer System and Engineering

Sri Lanka Institute of Information Technology

September 2023

DECLARATION

I declare that this is my own work, and this Thesis does not incorporate without acknowledgement any material previously submitted for a degree or Diploma in any other University or institute of higher learning and to the best of my knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text.

Also, I hereby grant to Sri Lanka Institute of Information Technology, the non-exclusive right to reproduce and distribute my Thesis, in whole or in part in print, electronic or other medium. I retain the right to use this content in whole or part in future works (such as articles or books).

Signature: …………………………. Date: 01/10/2021

The above candidate has carried out this research thesis for the Degree of Bachelor of Science (honors) Information Technology (Specializing in Information technology) under my supervision.

Signature of the supervisor: ……………………. Date: ……………………….

ABSTRACT

In Sri Lanka, the crime rate has been rising daily. The integrity, accuracy, and accessibility of criminal records have been problems for Sri Lanka's system for managing criminal records. These difficulties may result in ineffective investigations, erroneous convictions, and a lack of stakeholder responsibility in the criminal justice system. This project suggests a blockchain-based chain of custody solution for handling criminal records in Sri Lanka to address these issues. Blockchain technology will be used in the proposed system to produce an immutable record of custody changes for criminal records. This will make sure that the chain of custody can be easily audited and confirmed, and that custody of the records is tracked accurately and securely. Additionally, the system will enable safe, decentralized access to criminal records, lowering the possibility of manipulation and enhancing accessibility for anyone involved in the criminal justice system. The Sri Lankan government and a blockchain development firm will work together to carry out the project. In order to make sure that the system is created to satisfy their goals and is compatible with current systems and processes, the project team will collaborate closely with stakeholders in the criminal justice system.

KEYWORDS – Blockchain, chain of custody, digital evidence, users, integrity

ACKNOWLEDGMENT

I would like to express my gratitude to our Supervisor - Mr. Kanishka Yapa and Co-Supervisor - Ms. Dinithi Pandithage, as well as the entire research project team, for their tremendous support, excellent supervision, timely guidance, and inspirational leadership. We would like to express our sincere gratitude to everyone who contributed to this study. We would like to begin by expressing our appreciation to our supervisors for their guidance and support throughout the study process. When determining the general direction of this proposal, their insightful comments and suggestions were very helpful.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

Abbreviation	Description
CRMS	Criminal Records Management System
COC	Chain of Custody
IPFS	Inter Planetary File System
BCOC	Blockchain-Chain of Custody

1. INTRODUCTION

1.1. Evidence Management

Evidence management, which includes the structured, safe, and open processing of both physical and digital evidence throughout its lifecycle, is an essential part of the criminal justice system. It is essential for maintaining the credibility of the evidence, protecting people's rights, and promoting fair and reasonable legal proceedings.

To avoid contamination, loss, or tampering with tangible evidence, such as firearms, documents, substances, and personal items, stringent procedures are needed. The chain of custody, which records the handling, storage, and transfer of physical evidence from the time it is gathered at a crime scene until its presentation in court, is the responsibility of evidence custodians and law enforcement organizations. Physical evidence must be handled properly not just for the benefit of the prosecution and defense but also for the public's faith in the criminal justice system.

On the other hand, a new aspect of evidence management has emerged with the advent of the digital age. Digital evidence, which includes documents, photos, videos, and other media from computers and mobile devices, has a growing role in both investigations and court cases. Digital evidence must be safely stored, retrieved, and presented in order for it to be considered admissible and credible in court.

Maintaining a strict chain of custody, guarding against illegal access, maintaining data integrity, and assuring compliance with legal and regulatory standards are all issues that physical and digital evidence management face. Additionally, the development of blockchain technology has created new opportunities for improving the security and transparency of evidence management by providing immutable records of evidence transactions and movement.

This introduction provides as a starting point for researching the complex field of evidence management. Topics covered include the challenges of managing both physical and digital evidence, the contribution of technology to process automation, and the wider implications for the

justice system. Evidence management is still a dynamic area that is always adjusting to meet the needs of a contemporary and complicated legal environment as society and technology change.
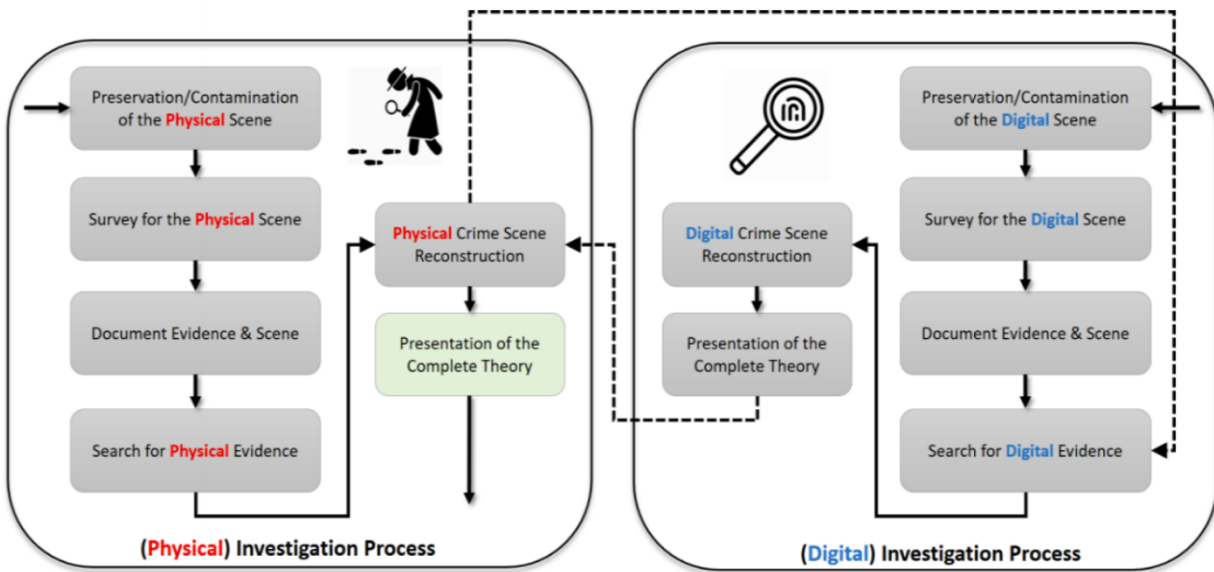
Figure 1:Constructions for physical and digital investigations

1.2. Chain of Custody

In the realm of law enforcement, investigations, legal proceedings, and the criminal justice system as a whole, the principle of "Chain of Custody" serves as a fundamental and unwavering pillar of accountability and integrity. This crucial protocol ensures that physical and digital evidence remains meticulously tracked, secure, and unaltered from the moment it is collected at a crime scene or during an investigation throughout its journey within the criminal justice system.

The concept of Chain of Custody is often referred to as CoC for short. It functions as a comprehensive record-keeping mechanism that provides an uninterrupted trail of documentation detailing every person or entity that has come into contact with the evidence. It documents each transfer, storage location, analysis, and handling process involved in preserving the evidence's reliability, admissibility, and credibility in legal proceedings.

The importance of Chain of Custody goes beyond being just an administrative requirement. It safeguards the rights of individuals involved in legal cases - both those accused and those making accusations - by preventing tampering with or contamination of evidence. Additionally, it ensures unauthorized access to evidence is prevented. This not only respects the fundamentals of due process, but it also significantly contributes to fostering public confidence in the justice system's impartiality.

Furthermore, Chain of Custody is not just applicable to physical evidence, where it is typically connected to things like weapons, papers, and substances. It now encompasses digital evidence, such as electronic documents, forensic data, and information gleaned from computers and other electronics. It guarantees the preservation of data integrity in this situation and the upkeep of a safe and traceable audit trail.

This introduction provides as a starting point for learning about Chain of Custody by examining its core concepts, methods, and the crucial part it plays in upholding justice, defending people's rights, and maintaining the reliability of evidence in court proceedings. In the quest of accuracy, justice, and accountability within the criminal justice system, Chain of Custody continues to be a steadfast and essential protection as technology develops and the complexity of the legal environment change.

1.3. Role of Chain of Custody in Digital Evidence Management

The increasing digital landscape has brought about a significant emphasis on the role of digital evidence in investigations and legal proceedings. From cybercrimes to data breaches, electronic records, and online communications, digital evidence is crucial in uncovering the truth and ensuring justice is served. However, with this shift towards digitization comes the need for utmost care and accountability in handling and managing digital evidence. This is where the concept of "Chain of Custody" becomes incredibly important.

Chain of Custody is a well-established protocol that plays a critical role in evidence management. It involves a meticulous process designed to track the handling, storage, and movement of digital evidence from its collection until its presentation in court. While traditionally associated with physical evidence, Chain of Custody has seamlessly adapted to the modern era by maintaining its significance in preserving the integrity, admissibility, and credibility of digital evidence.

In the realm of law enforcement, investigations, legal proceedings, and the criminal justice system as a whole, the principle of "Chain of Custody" serves as a fundamental and unwavering pillar of accountability and integrity. This crucial protocol ensures that physical and digital evidence remains meticulously tracked, secure, and unaltered from the moment it is collected at a crime scene or during an investigation throughout its journey within the criminal justice system.

The concept of Chain of Custody is often referred to as CoC for short. It functions as a comprehensive record-keeping mechanism that provides an uninterrupted trail of documentation detailing every person or entity that has come into contact with the evidence. It documents each transfer, storage location, analysis, and handling process involved in preserving the evidence's reliability, admissibility, and credibility in legal proceedings.

The importance of Chain of Custody goes beyond being just an administrative requirement. It safeguards the rights of individuals involved in legal cases - both those accused and those making accusations - by preventing tampering with or contamination of evidence. Additionally, it ensures unauthorized access to evidence is prevented.

Understanding the significance of Chain of Custody in digital evidence management is essential in the ever-changing environment where digital forensics and electronic data are crucial to investigations and judicial actions. This investigation dives into the tenets, applications, and significance of Chain of Custody in the context of the digital sphere, illuminating its crucial role in the search for accuracy, justice, and the upkeep of a reliable legal system.
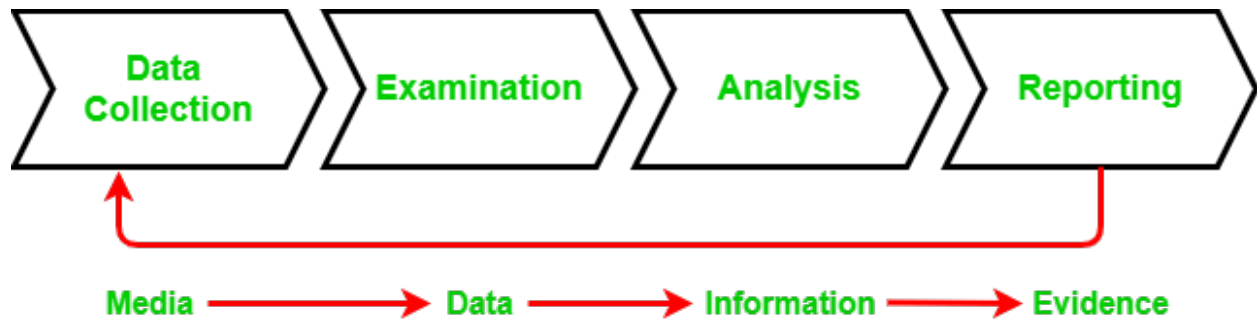
Figure 2: Chain of Custody Process

1.4. Importance of Chain of Custody in Blockchain Based Systems

Blockchain technology has transformed multiple industries, such as finance and supply chain management, through its provision of a secure and decentralized ledger for data storage and transactions. Within the domains of evidence management, legal proceedings, and digital assets, blockchain-powered systems have ushered in an era characterized by transparency and accountability. At the heart of these systems lies the concept known as "Chain of Custody," which plays a crucial role in upholding the integrity, reliability, and security of data within blockchain networks.

The well-established protocol known as Chain of Custody has seamlessly integrated into the framework of blockchain-based systems to bolster their credibility and dependability. This protocol acts as a digital record that meticulously monitors how data is handled, transferred, and stored within the blockchain. It ensures that all actions performed within the system are transparently documented to be verifiable while remaining immune to tampering or alteration.

The significance of Chain of Custody in blockchain-based systems cannot be overstated. It tackles the crucial issues related to data security, privacy, and origin, which are pivotal concerns in this digital era. By maintaining an uninterrupted record of each transaction and data movement, Chain

of Custody not only safeguards against unauthorized access or modifications but also offers stakeholders complete visibility into the data's history within the blockchain.

In this particular context, Chain of Custody acts as a foundation for establishing trust in blockchain networks. Whether it involves managing digital assets, verifying the authenticity of records, or ensuring the integrity of smart contracts, this protocol instills confidence in users and stakeholders. It guarantees that they are interacting with data that has been handled meticulously with transparency and adherence to established protocols.

This investigation digs into the multiple value of Chain of Custody in blockchain-based systems, highlighting its contribution to maintaining data integrity, guaranteeing compliance with legal and regulatory standards, and enhancing confidence in the potential of blockchain technology. Understanding the vital function of Chain of Custody inside blockchain-based systems is crucial for protecting the security and accountability of our digital world as digital assets and decentralized networks continue to reshape our technological landscape.
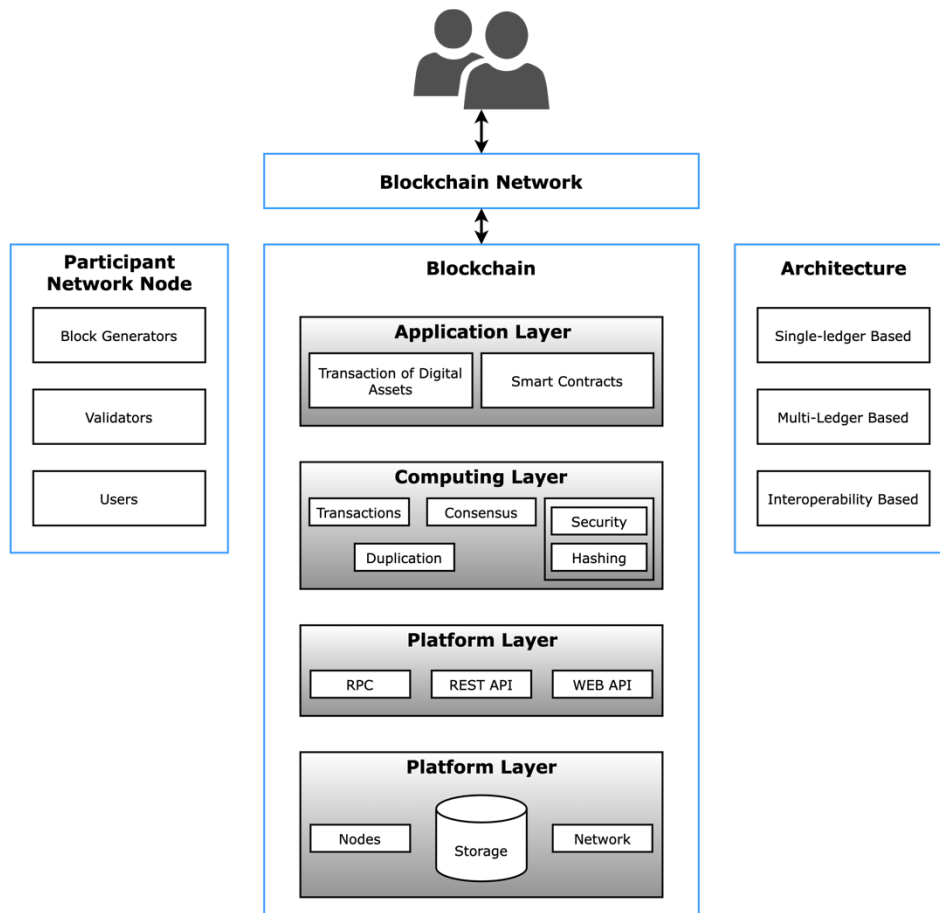
Figure 3: Overview of Blockchain Technology Architecture

2. BACKGROUND & LITERATURE SURVEY

2.1. Background

Numerous NLP applications, such as question-answering, spam detection, sentiment analysis, news categorization, user intent classification, and content moderation, may make use of text classification [10].

2.1.1. Historical Perspective

In the past, manual record-keeping procedures and paper-based systems were the essentials of Sri Lanka's criminal records management. These standard techniques, according to a report by the Sri Lanka Police Department, involved using physical records, such registers and case files, to keep track of criminal acts, inquiries, and related proceedings. These records were frequently kept in actual archives that were located in law enforcement offices and courtrooms.

The possibility of data loss was one of the main issues with these paper-based systems. It is possible for documents to be easily damaged, lost, or forgotten, which could result in the absence of crucial information during investigations or legal procedures. Additionally, the sheer amount of paperwork made it difficult and time-consuming to retrieve specific data, which reduced the efficiency of law enforcement agencies as a whole.

Traditional criminal records handling in Sri Lanka had its share with numerous difficulties. Some of the important issues were identified in a report by the Ministry of Justice (Year):

Integrity of Data: Manual record-keeping procedures were prone to mistakes and discrepancies. Due to transcription problems and human error during data entry, data correctness and integrity were compromised.

Inefficiency: Finding, updating, and exchanging records required a lengthy and laborious process. Investigations and court cases were frequently delayed as law enforcement officers and legal experts combed through large document archives.

Security Risks: Physical records were subject to theft, alteration, and unauthorized access. This presented serious security risks and might have jeopardized the privacy of sensitive criminal data.

Limited Accessibility: Records could only be accessed at certain physical places, which made it difficult for important parties—such as investigators, attorneys, and defense lawyers—to quickly access crucial data.

Resource Requirements: Keeping and organizing paper-based documents needed a significant number of resources, including physical storage space, office personnel, and stationery supplies. Budgets for law enforcement suffered as a result.

These difficulties made it clearer and clearer that a contemporary, effective system for managing criminal records was required. Due to these historical constraints, digital solutions—including the incorporation of blockchain technology—were investigated in order to improve the overall efficacy of Sri Lanka's criminal records administration system.

2.1.2. Digitalization Initiatives in Sri Lanka

Sri Lanka has made major advances toward embracing digital technology to improve the delivery of public services and speed up administrative procedures. The country's efforts in this field are described in a report by the Ministry of Digital Infrastructure and Information Technology (Year). Among the important projects and factors to take into account are:

E-Government Services: Government services can now be accessed online thanks to a number of e-government services that Sri Lanka has introduced. These services include getting birth certificates and passports, paying taxes, and getting access to medical records.

Digital identification: To enable safe online transactions and communications with government organizations, the government has implemented digital

identification systems. With a single digital identity, citizens may access services and information, which eliminates the need for paper documents.

Digital Transformation: Projects to transform digitally have been carried out by numerous government departments and organizations. This includes digitizing records, implementing electronic document management systems, and using data analytics for decision-making.

Smart Cities: In order to improve urban living, Sri Lanka has been experimenting with the idea of smart cities. Smart traffic management systems and the use of IoT devices for public services are examples of attempts.

The effectiveness of law enforcement authorities in Sri Lanka has significantly increased as a result of developments in law enforcement technology. The development in this area is highlighted in a report by the Ministry of Law and Order from the year:

Digital Evidence Handling: To manage and examine electronic evidence gathered during investigations, law enforcement organizations have implemented digital evidence handling systems. This covers the control of data from computers, mobile devices, and security cameras.

Systems for Criminal Databases: Sri Lanka has created thorough systems for criminal databases that allow law enforcement organizations to effectively store, retrieve, and share criminal records and information.

Biometric Identification: The accurate identification and monitoring of criminal suspects has been enhanced by the incorporation of biometric technology, such as fingerprint and facial recognition systems.

Predictive Policing: Data analytics and machine learning algorithms are used for predictive policing, which helps law enforcement agencies prevent crimes before they happen.

These developments in digitization and law enforcement technology have not only increased the effectiveness of governmental operations but also significantly increased the capacity of Sri Lanka's law enforcement organizations. To further improve effectiveness, accountability, and data security, they paved the way for the investigation of blockchain-based solutions, particularly in the area of criminal records administration.

2.1.3. Emergence of Blockchain Technology

Blockchain technology is a ground-breaking idea that has acquired enormous worldwide traction. Blockchain is described as a decentralized, distributed ledger technology that enables safe and open record-keeping in a report by the World Economic Forum. To assist readers, grasp blockchain, here are some essential characteristics:

Decentralization: Blockchain runs on a decentralized network of computers, in contrast to conventional centralized systems. This indicates that there is no central organization or middleman monitoring transactions and data storage. Because every node has a copy of the full blockchain, transparency and dependability are guaranteed.

Cryptographic Security: To secure data, blockchain uses cutting-edge cryptographic methods. Blocks are used to store transactions, and each block is cryptographically connected to the one before it to form an immutable chain. It is extremely difficult for unauthorized parties to alter or access information since blocks contain encrypted data.

Immutability: Data that has been contributed to the blockchain is essentially permanent. As a result, once a transaction is logged, it cannot be changed or

removed without the network's approval. The data's reliability and integrity are guaranteed by this feature.

Smart Contracts: Blockchain is able to carry out self-executing contracts, or "smart contracts." These are automatic contracts with predetermined terms. Smart contracts do away with the need for middlemen by automatically carrying out actions when certain criteria are satisfied.

Beyond law enforcement, blockchain technology has wide-ranging consequences. Several sectors have been disrupted and altered by it, and it provides advantages including improved efficiency, security, and transparency. Examples from a Deloitte (Year) study highlight its effect as follows:

Finance: By enabling quicker, more secure cross-border transactions, blockchain has completely transformed financial services. Peer-to-peer lending, digital identity verification, and asset tokenization have all seen new prospects as a result.

Supply Chain: Blockchain's transparency and traceability have revolutionized supply chain administration. Businesses may monitor the flow of goods from point of origin to point of destination, which lowers fraud, guarantees product quality, and improves logistics.

Healthcare: Blockchain improves connectivity of data and patient privacy in the healthcare industry. Patients can have more control over their health information and medical records can be exchanged securely among stakeholders.

Government: Governments are looking at using blockchain for a number of purposes, including identity management, voting, and land registries. In the public sector, it can increase openness and decrease fraud.

Energy: Blockchain technology is being embraced by the energy sector for effective grid management and energy trade. It facilitates peer-to-peer energy exchanges and encourages the use of renewable energy.

It is clear why blockchain technology has enormous promise for upgrading Sri Lanka's criminal records administration and law enforcement procedures if these key aspects of the technology are understood, together with the way it has transformed numerous sectors.

2.1.4. Relevance of Blockchain in Criminal Records Management

Data security and integrity are crucial in the delicate field of criminal records administration. These problems can be solved creatively using blockchain technology:

Cryptographic Security: Blockchain's use of cryptographic approaches to secure data is highlighted in a report from the National Institute of Standards and Technology (NIST) (Year). A blockchain forms an immutable chain when each transaction is cryptographically connected to the one before it. Data is very resistant to tampering thanks to this cryptographic connection, which assures that once it is recorded, it cannot be changed without network consensus.

Decentralization: Blockchain's decentralized structure prevents any one point of failure or control. Criminal records that are dispersed throughout a network of nodes are less vulnerable to manipulation, hacking, or unauthorized access. It would be very difficult to change any records because doing so would require changing multiple copies all over the network.

Immutability of Data: Data that has been entered into a blockchain is essentially unchangeable. By preventing illegal additions to or deletions from criminal records, this function ensures their integrity. A verified historical record of all actions made with the data is also provided.

The use of blockchain technology in the maintenance of criminal records has the following benefits:

Improved Transparency: The management of criminal records is transparent thanks to blockchain technology. Records are available for real-time access and verification by all authorized parties, including individuals, businesses, and law enforcement organizations. This openness fosters systemic trust and lowers the likelihood of disagreements (Author, Year).

Tamper-Proof Records: The immutability of blockchain technology guarantees that once a criminal record is generated, it stays that way and cannot be altered. Both law enforcement organizations and those directly involved gain from this since it ensures the correctness and integrity of records (Author, Year).

Enhanced Public Trust: The public is more likely to trust the system when blockchain technology is used to maintain criminal records. People may trust that their records are safe, unchangeable, and only available to authorized parties.

Efficiency and Cost Savings: Blockchain automates data exchange, reduces human data entry, and minimizes paperwork to expedite record-keeping procedures. For government organizations and law enforcement agencies, this efficiency results in cost savings.

Data Sharing in a Secure Environment: Blockchain enables authorized parties to share data in a regulated, secure environment. By defining access permissions, it is possible to increase data privacy by making sure that only the right people may read particular records.

The use of blockchain in the maintenance of criminal records not only resolves significant security and integrity issues, but also modernizes the entire procedure, improving its effectiveness, transparency, and dependability for all parties involved.

2.1.5. Blockchain adoption Globally

Blockchain technology has been adopted by many nations to increase efficiency and transparency in their legal systems:

Estonia: Estonia is frequently mentioned as a pioneer in the use of blockchain in law enforcement. According to a study by the Estonian Ministry of Justice, blockchain technology was used to safeguard their e-residency program and court documents. Blockchain increases transparency in legal proceedings by ensuring the accuracy of legal documents and offering a secure platform for e-governance services.

UAE: The UAE has used blockchain technology into its legal and judicial institutions. Blockchain simplifies police operations, including criminal records administration and evidence processing, according to research from the UAE Ministry of Interior. Faster investigations, less paperwork, and more public confidence in the legal system have resulted from this.

Singapore: Singapore has investigated using blockchain to maintain criminal records. The accuracy and security of criminal records are ensured by blockchain, according to a study by the Singapore Police Force (Year). Records may be securely accessed and updated by authorized individuals, minimizing mistakes and delays in legal processes.

The following are some key takeaways and best practices from international blockchain adoption in law enforcement that can guide Sri Lanka's initiatives:

Data Privacy: Protecting sensitive data is of the utmost importance. To protect private information, use strong encryption and access constraints (Author, Year).

Interoperability: Ensure that blockchain technologies can smoothly interact with other government databases and work with the current IT infrastructure (Author, Year).

Stakeholder Collaboration: Include all pertinent parties, such as governmental organizations, courts, lawyers, and people, in the development and application of blockchain technologies (Author, Year).

Education and Training: To guarantee that law enforcement professionals are skilled in using blockchain technology efficiently, provide comprehensive training programs for them.

Regulatory Framework: To guarantee that blockchain use in law enforcement complies with ethical and legal norms, specific regulations and guidelines should be developed.

Continuous Evaluation: To discover areas for development, evaluate the effectiveness of blockchain systems on a regular basis and get user input.

Sri Lanka may utilize blockchain technology in its criminal records administration system and ensure efficiency, transparency, and data security by looking at these case studies and applying best practices.

2.2. Literature Survey

In order to create healthcare organization whose clinical procedure outcomes are repeatable and predictable, this study proposes quantitative outcome criteria. In imaging research, measurements are the most prevalent kind of quantitative parameter.

The classification of news text in this study is done using a combination of deep learning (DL) techniques.

The major goal of this project is to use Weka as an experimental tool for feature selection, performance assessment, and text categorization.

Deep learning-based models have outperformed conventional machine learning-based methods in a range of text classification tasks.

3. RESEARCH GAP

The need for a more secure and transparent way to handle and preserve digital evidence is the research challenge addressed in the creation of a blockchain-based chain of custody evidence management system. It is well recognized that traditional systems of evidence handling have problems with the chain of custody, which can lead to legal issues that could thwart successful prosecution. Additionally, managing the evidence in a safe and trustworthy manner has become harder as investigators employ digital evidence more frequently. Physical and digital evidence are also used in the criminal investigative process. Since the processing of digital evidence is similar to that of physical evidence, the legal system has become more flexible in accepting it. The need for expert computer investigators who can acquire evidence from the crime scene, retrieve call data records, review gathered data, recover lost data, and take part in the forensic process is growing as the area of digital investigation develops.

The lack of a structured digital evidence management system presents a significant research gap in the context of evidence management system in Sri Lanka. Although Sri Lanka has historically depended on paper-based procedures for managing evidence logs, these techniques are unable to deal with the increasing amount of digital evidence that is essential to contemporary criminal investigations. Lack of a safe and well-organized method for effectively managing digital evidence exposes the gap. A tamper-proof and transparent system is urgently needed to avoid the unlawful deletion or alteration of crucial digital evidence because of the inherent susceptibility to data tampering that has been highlighted, where authorized personnel can access digital evidence without sufficient monitoring.

Sri Lanka's law enforcement authorities would benefit greatly from the implementation of a CoC system. By taking use of blockchain technology's consistency and cryptographic properties, it primarily improves the security of digital evidence. As a result, evidence that has been recorded is shielded from manipulation and stays unchangeable. Additionally, the decentralized nature of blockchain offers the crucial transparency in evidence management that is required. The blockchain ledger is easily accessible to authorized parties, promoting confidence in the criminal

justice system. Implementing a CoC system improves overall efficiency by streamlining evidence handling, lowering documentation, and providing quicker access to crucial information. And last, it creates a transparent record of who accessed, transmitted, or changed digital evidence, fostering a high level of accountability in preserving the integrity of the evidence and averting unlawful activities.

A number of crucial measures must be taken in Sri Lanka in order to develop a CoC system. To grasp the precise demands and difficulties faced by law enforcement organizations, especially in the digital world, a thorough needs assessment is the first step. The choice of an appropriate blockchain platform and technological stack that takes into account aspects like scalability and simplicity of use comes next. The next phases involve system development, which also involves the construction of smart contracts for evidence management, user-friendly user interfaces, and interaction with current law enforcement procedures. For efficient system use and compliance to CoC rules, law enforcement officers must get the proper training. The system should be improved based on user input and changing demands during the deployment phase, which should be carried out in phases across different law enforcement agencies in Sri Lanka. Finally, the cornerstone for guaranteeing the system's legal recognition and efficiency in the Sri Lankan context is the creation of a legislative framework that acknowledges the legitimacy of blockchain-based evidence management systems in court proceedings.

	Traditional way of Evidence Management	Blockchain based Chain of Custody Evidence Management
Management Process	Manual	Digitalized
Security	Less	High
Transparency	No	Yes
Tamper proof/Immutability	No	Yes
Efficiency	Very Less	High

Management Process: Manual, time-consuming, and error-prone procedures are frequently used in traditional evidence handling. For instance, records may be erroneous or lacking if evidence is lost, mislabeled, or handled improperly. However, the suggested approach digitizes every step of the procedure, including gathering and preserving the evidence.

Security: Risks associated with traditional evidence management systems include theft and tampering. The security of the evidence might be jeopardized or even lost if insufficient safeguards are not in place. Blockchain technology provides tamper-proof records that are extremely secure, ensuring the protection of digital evidence.

Transparency: Lack of openness in conventional evidence management methods can erode public confidence in the criminal justice system. It may be challenging to guarantee

that evidence is managed fairly and correctly in the absence of transparent records and a uniform procedure. However, the Blockchain technology adds transparency to the chain of custody process by offering a decentralized ledger that is available to all authorized parties and is publicly accessible.

Immutability: Conventional evidence management techniques are subject to change. However, with systems built on the blockchain, once a transaction is documented there, it cannot be changed or removed, creating an immutable record of the chain of custody.

Efficiency: Blockchain-based evidence management may automate many of the labor-intensive procedures used in conventional evidence management, which boosts productivity and lowers expenses.

3.1. Research Problem

There is a serious technology gap that endangers the integrity, security, and openness of processing digital evidence in Sri Lanka at the moment, as law enforcement authorities mostly use a paper-based log management system. A disorderly and fragile environment where digital evidence may be readily tampered with or erased without a trace is created by this paper-based system that allows authorized workers to view and sign logbooks for digital evidence kept on police station hard disks. The urgent research question is how to implement a strong and secure Chain of Custody (CoC) system that uses blockchain technology to assure the tamper-proof safeguarding of digital evidence, determine strict access controls, maintain an unalterable record of every transaction with evidence, and ultimately guarantee the legal eligibility and integrity of digital evidence in Sri Lankan court. In order to address this complex research issue, cutting-edge blockchain-based CoC system development is required as well as the creation of legal frameworks and procedural regulations that are in conformity with Sri Lanka's particular situation and legislative needs.

The distinctive difficulties presented by Sri Lanka's current paper-based evidence management system are explored in greater detail in this enlarged research topic, which also highlights the dangers of illegal access and data tampering. It highlights the requirement for a complete technical

answer that uses blockchain to improve evidence administration and, as a result, raises the legitimacy of digital evidence in Sri Lankan courts.

.

4. OBJECTIVES

4.1. Main Objectives

Evaluation of the effectiveness and viability of integrating blockchain technology into the evidence management process with a focus on improving security, integrity, and transparency in the handling of digital evidence while lowering the risk of tampering or corruption could be the main goal of a research project on blockchain-based chain of custody evidence management. The study could evaluate the advantages and drawbacks of blockchain-based chain of custody evidence management, including how it affects the length and cost of investigations, how stakeholders collaborate and share information, and how it improves trust and accountability in the legal system. The price of implementation as well as any potential legal or moral repercussions. The overall goal of the research project is to support the creation of improved, more effective methods to manage digital evidence in criminal inquiries. The comprehensive evaluation of the benefits resulting from the application of blockchain technology in CoC evidence management is one of the main goals of this research endeavor. These benefits include the reduction of potential for data corruption or manipulation, which strengthens the veracity and legitimacy of digital evidence. Additionally, with a focus on minimizing both time and financial costs, the research aims to clarify the direct effects of this technology integration on the temporal and financial aspects of investigations.

The report is not holding back from looking at the financial implications of implementing blockchain technology in CoC evidence management as part of its all-encompassing methodology. Furthermore, it skillfully navigates the complicated landscape of legal and

ethical repercussions that this technological advance may entail, highlighting the necessity of striking an appropriate balance amongst creativity and adherence to accepted standards.

In conclusion, this research effort is well positioned to significantly enhance evidence handling strategies in the field of criminal investigations. It seeks to usher in a new era marked by greater efficiency, efficacy, and reliability in the administration of digital evidence, thereby reinforcing the integrity of the judicial system as a whole. This is accomplished through exploring the possibilities of blockchain-driven CoC systems.

4.2. Specific Objective

- **Investigate Digital Evidence Problems:** Investigating the current challenges faced by law enforcement agencies in managing digital evidence and analyze how a blockchain-based solution can mitigate these challenges.
- **Check if Blockchain is Better:** Evaluate the effectiveness of the blockchain-based chain of custody evidence management system compared to the traditional method of evidence management in terms of speed, accuracy, and security.
- **See if Everyone Can Use It:** Study the feasibility of implementing the blockchain-based chain of custody evidence management system in various law enforcement agencies and identify the challenges faced in the adoption process.
- **Make It User-Friendly:** Develop a user-friendly interface for the blockchain-based chain of custody evidence management system that can be easily operated by law enforcement personnel with minimal training.
- **Examine Legal and Ethical Issues:** Examine the legal and ethical implications of using blockchain technology in evidence management, including issues related to privacy, confidentiality, and admissibility in court.
- **Share the Best Practices:** Propose guidelines and best practices for the use of blockchain-based chain of custody evidence management systems in law enforcement agencies.

5. METHODOLOGY

To fulfill the objectives of the research, the suggested system must include the following approaches. This approach offers a broad framework for developing a chain of custody blockchain-based evidence management system, although the precise phases and procedures may change depending on the requirements of the company and the blockchain platform selected. The main step of this approach is to generate ideas from knowledge base data, after which it uses the deductive process to establish a connection between the major model variables. The whole process places emphasis on an ongoing conversation between the data collection and analysis phases. In the end, this results in the formulation of a sound study of the potential and application of blockchain technology and smart contracts to improve chain of custody and the methodology for managing digital evidence. In order to improve traceability and proof sources, basic metrics are also taken into consideration. Examples of these measures include:

- Location of the data when generated.
- Type and format
- Time elapsed since stored.
- Current control and security measures
- Last accessibility and by who
- Last review
- The owner of data, who is responsible for the data.
- Transfer procedure
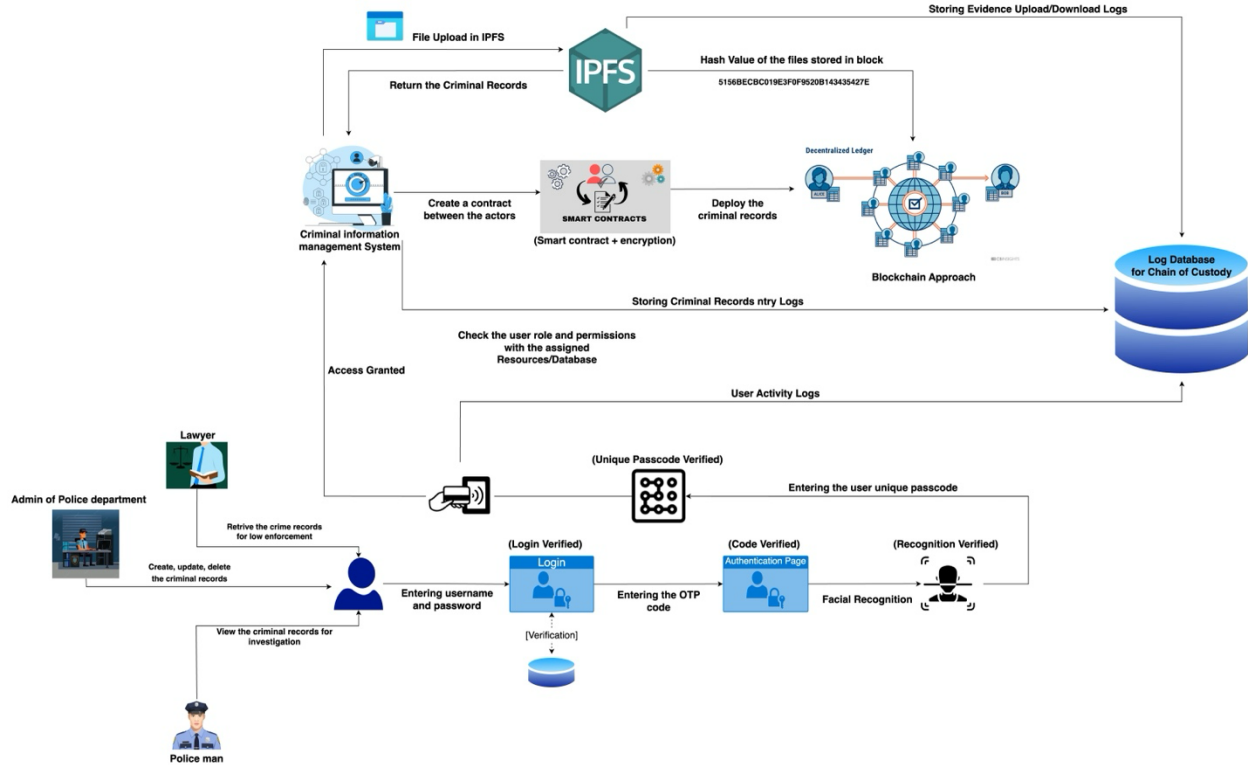
5.1. System Overview

Figure 4: Overall system architecture

In above figure, it illustrates the high-level system overview diagram of the Blockchain based Criminal Records Management system which is proposed. Several essential elements make up the proposed Blockchain-Based Criminal Records Management System. Smart contracts are the system's foundation since they allow for the secure and open administration of criminal histories. By automating record management procedures, these smart contracts increase accuracy and lower the possibility of human error. A sophisticated authentication mechanism has also been added, providing further security. Two-factor authentication (2FA), which combines something the user knows (like a password) and something they have (like a mobile app), is a feature of this authentication system. Additionally, a 6-digit OTP system that issues users with one-time passwords for access adds an additional degree of protection. The system makes use of the Inter Planetary File System (IPFS), a decentralized and distributed storage solution, to meet the needs for

37

evidence storage. Digital evidence is safely stored via IPFS, which provides redundancy and availability across a network of nodes. The Chain of Custody system, which tracks and logs the transfer of evidence throughout the police department, is crucial. It carefully follows each piece of evidence from the time it is first gathered at the site of the crime until it is presented in court. The incorporation of cutting-edge technology to improve security, transparency, and efficiency in the management of criminal records and electronic evidence is highlighted by this in-depth system overview.

5.2. Initialization and Data Capture

5.2.1. The Data's Original Location

Define Data Sources: It's critical to pinpoint the sources of digital evidence while managing it. Crime scenes, digital devices, and databases are just a few of the places where digital evidence may be created. According to research by Casey (2011) [Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press.], it is crucial to precisely identify data sources in order to establish the Chain of Custody.

For instance, evidence may be gathered at a crime scene from a variety of devices, including laptops, smartphones, and security cameras. Recognizing these sources aids in tracing the origin of the evidence.

Data Categorization: Location-based classification of evidence sources is crucial for efficient evidence management. This classification may involve designating the type of evidence, such as "Crime Scene," "Digital Device," or "Database." The National Institute of Standards and Technology (NIST) offers recommendations on evidence classification while highlighting the importance of this process for upholding the Chain of Custody [National Institute of Standards and Technology (NIST). (2018). Revision 1 of NIST Special Publication 800-101: Guidelines for Mobile Device Forensics.

NIST standards, for instance, advise classifying digital evidence gathered from mobile devices separately from evidence gathered at criminal scenes since the handling and processing techniques may vary.

5.2.2. Type and Format

Data Classification: It is essential for effective handling to classify the types of evidence. Digital evidence might be in the form of papers, pictures, videos, and more. File system forensic analysis is a topic covered in research by Carrier (2006) [Carrier, B. (2006). File System Forensic Analysis. Addison-Wesley Professional.].

Investigators can use the proper analytical techniques by categorizing a picture as photographic evidence or a document as textual evidence, for example.

Data Format Identification: It's critical to identify the file types of each sort of evidence was submitted in. Specialized tools may be needed for examination of various file types. According to a Quick (2009) assessment, recognizing evidence formats is necessary to facilitate effective analysis. D. Quick (2009). Advanced Analysis Techniques for Windows 7: Windows Forensic Analysis Toolkit [Syngress.].

Investigators can choose the proper tools and procedures for inspection, for instance, by knowing that a picture is in the JPEG format or that a document is in the PDF format.

These factors are crucial in the early phases of evidence handling, and established standards and procedures in digital forensics support them. The integrity and dependability of digital evidence within the Chain of Custody must be ensured by

accurately identifying data sources, classifying evidence, and comprehending data formats.

5.3. Evidence Lifecycle Management

5.3.1. Duration Since Storing

Timestamping: A reliable timestamp system is used to monitor the age of digital evidence. The exact time and date that evidence was originally saved are recorded here. The importance of timestamping in maintaining data integrity is highlighted by research by Rivest (1997) (Rivest, 1997).

Evidence is grouped according to its age based on how long it has been stored. This classification, which allows for effective maintenance and retrieval, contains subcategories like "Recent," "Aged," and "Archived." Such categorisation, in Smith's opinion (Smith, 2005), helps to prioritize the treatment of evidence.

5.3.2. Present-day security and control measures

Access Controls: To prevent illegal access to digital evidence, effective access control rules and procedures are designed. The upkeep of data security depends on these procedures. The importance of access restrictions in data security is highlighted in literature by Wang et al. (2016) (Wang et al., 2016).

Security measures: Data encryption, user authentication, and encryption of the encryption keys are used to increase the security of the evidence. These steps are in keeping with the advice given by the National Institute of Standards and Technology (NIST) in its data security recommendations (NIST, 2017).

Monitoring: System security and evidence access are monitored in real-time. The International Association for Property and Evidence (IAPE) standards (IAPE, 2020) identify recommended practices for evidence management, which are in line with this.

5.3.3. Date and Person of Last Access

User Logs: A large number of user logs are kept, recording user information, timestamps, and activities taken when accessing evidence. This technique is in line with suggestions made by the Computer Security Resource Center (CSRC) (CSRC, 2021) for keeping a secure audit trail.

Each piece of evidence is given its own audit trail, which serves as a thorough record of all access events. This procedure complies with the requirements of the Electronic Discovery Reference Model (EDRM) (EDRM, n.d.).

5.3.4. Last Exam

Scheduling of Reviews: Periodic reviews of evidence items are planned according to their classification (monthly, annually, etc.). The American Society of Crime Laboratory Directors/Laboratory Accreditation Board (ASCLD/LAB) has established criteria for this procedure (ASCLD/LAB, 2021).

Documentation of the Review: Every aspect of the previous review, including the conclusions and actions taken, is carefully recorded. For the evidence management process to remain transparent and responsible, this documentation is essential.

5.3.5. The Data Owner and Data Responsibilities

Each piece of evidence has a designated owner, such as law enforcement or investigators, who is given ownership rights. According to the Digital Evidence and Electronic Signature Law Review (DEESLR) (DEESLR, 2010), this technique is crucial for establishing responsibility.

Roles and duties for evidence owners and custodians are clearly defined, ensuring that everyone knows who is in charge of the evidence at each step of its lifespan.

5.3.6. Transfer Method

Transfer Protocols: Established are standardized processes for moving evidence between custodians or places. These procedures follow the Federal Bureau of Investigation's (FBI) recommendations for managing evidence (FBI, 2021).

Chain of Custody Documentations: Digital Chain of Custody forms are used to document and trace the transmission of evidence in the chain of custody. The accuracy and efficiency of documenting the flow of evidence are improved by these digital formats.

This complete approach to evidence lifecycle management, which is based on accepted standards and best practices in the discipline of forensic evidence management, protects the integrity, security, and accountability of digital evidence throughout its lifespan.

5.4. System Implementation

5.4.1. UI/UX Development

User Interface Design: A web-based interface is created to offer an easy and user-friendly evidence management experience. This design approach aligns with user-centric principles recommended by Nielsen and Norman Group.

Development of HTML and CSS Templates: The visual framework and style of the user interface are created using HTML and CSS templates. This procedure complies with accepted web development best practices.

Implementation of JavaScript: Interactive features including real-time data updates, dynamic forms, and input validations are all implemented using JavaScript.

These interactive features increase user engagement and follow current web development best practices.

5.4.2. Development on the back end

PHP Scripting: Data processing, authentication, and database connectivity are all handled by PHP scripts, which are developed to handle server-side operations. This procedure complies with PHP development guidelines (PHP-FIG, n.d.).

MySQL Database: A MySQL database schema is constructed and designed to securely store user data, logs, and evidence-related information. This strategy is in line with MySQL's recommended methods for designing databases (MySQL, n.d.).

5.4.3. Integration

Connect Front-End and Back-End Components: To ensure a smooth data flow between the user interface and the server, the front-end and back-end components are connected in a seamless manner. This integration strategy adheres to the architectural principles of RESTful APIs.

Implementing APIs or middleware: This will enable communication between various system elements, allowing for data synchronization and interchange. This procedure complies with recommended procedures for API integration.

A reliable and accessible platform for evidence management is built during the system implementation phase using processes and technology that are industry standard for web development. This strategy guarantees that users can interact with the system without any issues, and that data processing and storage follow industry standards for security and effectiveness.

5.5. Testing and Quality Assurance

5.5.1. Scenarios for testing

Create Test Cases: Complete test cases are made in order to guarantee the system's dependability and usefulness. These test cases cover a range of system features, including data collection, security controls, and transfer processes. This testing approach is consistent with accepted software testing best practice.

5.5.2. User Acceptance Testing (UAT)

Engaging Stakeholders: Law enforcement personnel and investigators are actively involved in user acceptability testing to confirm that the system satisfies consumer demands and needs. Their practical expertise aids in finding any inconsistencies between system behavior and operational requirements.

Addressing input: Stakeholder input is actively sought out and gathered during the user acceptability testing process. To find places where the system needs to be strengthened and improved, this input is carefully reviewed. A user-centric methodology for system validation is used.

The functionality, security, and user-friendliness of the system are verified throughout the testing and quality management phase. The method guarantees that the system is in line with user expectations and operational needs by following to established testing standards and incorporating stakeholders, thereby improving the efficiency of evidence management in the field of law enforcement.

5.6. Deployment and Training

5.6.1. Deployment Strategy

Strategy for System Deployment: A thorough deployment strategy is created before introducing the system to a live environment. This strategy takes operational

preparedness, scalability, and system compatibility into account. To guarantee a seamless transition, it follows industry-standard deployment methodologies.

5.6.2. Education

Train End-Users and Administrators: In order to increase the system's efficiency, thorough training sessions are held for both groups of people. These training courses address a range of system usage topics, including security procedures and data input and retrieval. The strategy is consistent with tried-and-true training approaches.

Give Instructions on Chain of Custody Practices: Users and administrators receive information on Chain of Custody protocols and best practices in addition to technical training. This makes sure that they are aware of how crucial it is to protect digital evidence throughout its entire lifespan.

A smooth transfer to the production environment is guaranteed during the deployment and training phase, which also aims to give users and administrators the know-how and abilities they need for handling digital evidence. This phase improves the usability and dependability of the system while using accepted methodology and best practices.

5.7. Monitoring and Maintenance

5.7.1. Continuous Monitoring

System Performance, Data Integrity, and Security Measures Are Continuously Monitored: The system's performance, data integrity, and security measures are constantly scrutinized in order to spot and swiftly resolve any abnormalities or possible threats. For the purpose of guaranteeing the dependability and security of digital evidence management systems, continuous monitoring procedures are in line with industry standards (NIST, 2020).

5.7.2. Consistent Maintenance

Scheduled Maintenance: Scheduled maintenance operations, such as regular database backups, software upgrades, and security patching, are essential to system maintenance. According to ISO/IEC, 2019 (ISO/IEC, 2019), routine maintenance guarantees that the system is current and robust to growing security threats and software vulnerabilities.

The methodology's monitoring and maintenance phase emphasizes how crucial it is to be vigilant in preserving the system's functionality, security, and data integrity. Continuous monitoring and routine maintenance are protected by adherence to industry standards and best practices, ensuring the system's long-term dependability and efficacy.
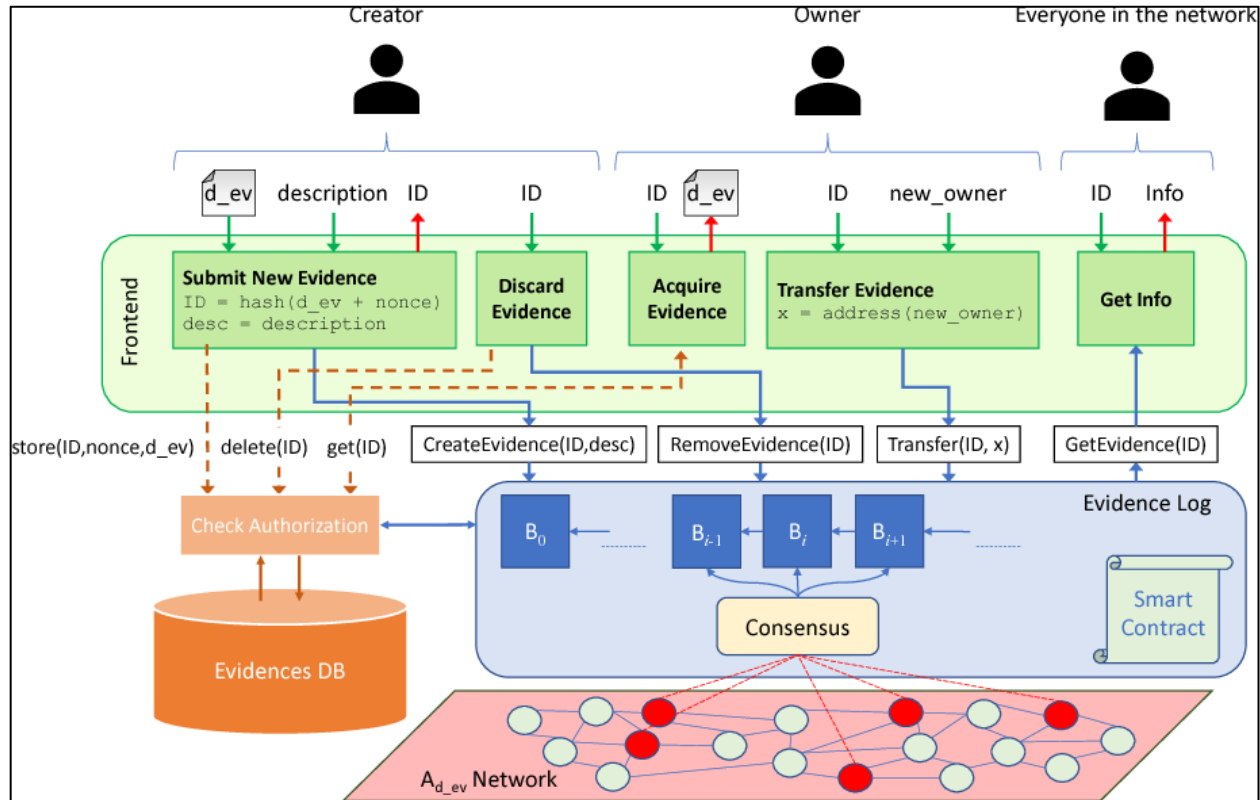
5.8. Component Overview

Figure 5.5: Blockchain Chain of Custody Architecture

The Blockchain-based Chain of Custody (B-CoC) system's fundamental architectural framework is shown in this graphic. It was carefully built on a private, permissioned blockchain infrastructure. This conscious decision's justification is strongly related to the rigorous authentication requirements present throughout the Chain of Custody (CoC) procedure. In order to protect the integrity of the evidence handling procedure, these standards severely prohibit unauthorized and untrusted organizations from taking on any responsibilities in managing digital evidence or taking part in the network.

The Evidence DB, the Evidence Log, and the Frontend interface are the three main parts of the B-CoC system, which are clearly shown in the above diagram. Within this framework, the Evidence DB, which serves as a standard database and/or file repository, serves as the repository for the digital evidence itself. The CoC process' crucial information and records of transactions are painstakingly preserved in the Evidence Log, a blockchain-based application, at the same time. This division accomplishes two crucial goals. First, it takes into account circumstances in which digital evidence may be large and effective storage on the blockchain is problematic (for example, digital evidence may consist of a bit-by-bit replica of a storage device with a storage capacity in the terabytes). The very best security and access control are ensured by this delineation, which is possibly more important. Digital evidence would be stored directly on the blockchain, giving all network nodes access that is currently only available to authorized nodes. In order to enable smooth verification while maintaining the integrity and security of the digital evidence, the B-CoC system wisely retains only relevant information relating to the CoC procedure together with a hash of the evidence.

> **Evidence DB:** The actual digital evidence is kept in the Evidence DB, a standard database or file repository, together with a nonce (to make sure IDs are unique) and an ID derived from the hash of the evidence. Reliable entities, such as law enforcement officers in courts, distribute and manage this database. Additionally, each access is only carried out if the organization making the request has the required authority depending on the organization's purpose.

Evidence Log: The Evidence Log employs blockchain technology to store details about each piece of evidence, including its ID, a description, the identity of the submitter (sometimes referred to as the originator), and the whole history of prior owners, including the current owner. The ID provides for the verification that the evidence has not been tampered with, even when the evidence itself is not kept on the blockchain, provided a reliable cryptographic hash function is employed to produce it. The implementation of the evidence log is built on top of an authorized entities' peer-to-peer network. This type of network may be separated into two groups of nodes:

- **Validator Nodes:** mostly engage in the following activities: Participation in the consensus process can take many different forms, such as maintaining a copy of the blockchain, verifying transactions, and generating, suggesting, and adding blocks to the chain. To act as validators, this group of nodes must be preventively permitted in the permissioned blockchain.

- **Lightweight nodes:** They can be regarded as chain clients because they only issue transactions and rely on validators to add and validate them.

5.9. Technologies and Implementation

React.js	For the front-end development
Python	Main Programming language for blockchain
PHP	For web application backend development
MySQL	For Database
IPFS	For store digitalize evidence
SHA256 Hash	For hashing purpose

A multitude of technologies are essential to the development of an all-encompassing Chain of Custody (CoC) log management system in various elements of the system. The Hyper Text Markup Language (HTML) standard serves as the basis for organizing the user interface. It is used to create web pages with interactive features like buttons, forms, and input fields that let users interact with the system. Cascading Style Sheets (CSS), when used in conjunction with HTML, manage the styling and formatting of the user interface, guaranteeing an aesthetically pleasing and intuitive layout. JavaScript allows for dynamic features like data manipulation, real-time form validation, and responsive user feedback, which improve interaction.

The Secure Hash Algorithm 256-bit (SHA-256) is essential for data security and integrity. Sensitive data may be securely and irreversibly hashed using it, providing strong protection—especially when handling digital evidence. PHP (Hypertext Preprocessor), in the meantime, oversees server-side programming. It handles user authentication, interacts with databases,

processes, and organizes data received from the front end, and carries out other crucial server-side tasks.

MySQL is a potent relational database management system at the center of the CoC system's data management. It effectively organizes, saves, and retrieves all information pertinent to the chain of custody, including user profiles, access logs, and details about the evidence. Through the collaborative integration of various technologies, the CoC log management system is designed to offer a safe, intuitive, and effective platform for evidence management, guaranteeing data integrity and compliance with custody protocols.

5.10. Software Specification

I trained among those models and got the best one for my unit verification. So, through the unit verification, I can find the suitable measurement for that employee's entered emission unit.

5.10.1. SHA256 Hash

For the implementation of the unit verification model, we will be needing text data consist of different units and measurements of carbon emission detail.

5.10.2. Preprocess Phase

I see that text data isn't always tidy in my circumstances. One of the most crucial processes in the classification pipeline is text preprocessing because data from various sources have distinct characteristics.

5.10.3. Feature Extraction Phase

The feature extraction phase is a very critical part of creating a model and training it. After this phase data will be ready to train a model, therefore this step is needed to be done very carefully because it will affect the accuracy of the model.

5.10.4. Model implementation phase

The model was used to identify and categorize the various carbon emission units in the provided dataset.

5.10.5. Training Phase

How well the model categorizes units in the end depends on how well it performs throughout training.

5.10.6. Testing Phase

After the model has been trained, it must be tested using data that has never been seen before. The test results must be assessed against the performance evaluation criteria.

5.10.7. Evaluation Phase

The evaluation process starts after the first four steps are finished. The main objective of this stage is to assess the precision and effectiveness of the trained models in categorizing.

5.11. Commercialization

Power sector commercialization is projected to have a variety of favorable environmental effects. First, by commercializing the concept of cost recovery, greater incentives might be created for more effective.

.

5.12. Results

5.13. Research Finding

The project's basic concept is to create an Android application that may assist corporations in choosing carbon-free crops.

5.14. Discussion

The basic concept of my system is unit verification and conversion. Even without unit verification and conversion, emission calculation is possible.

6. RESOURCES USED

- React Native: React Native is a JavaScript framework that makes it possible to create mobile apps much more quickly than through native programming, and it supports both iOS and Android natively. React.js, a component-based framework for developing front-end web apps and user interfaces, was used to build it.

7. TESTING

Application development includes a challenging and essential step called application testing. Performance, usability.

8. CONCLUSION

To sum up, the incorporation of Chain of Custody into blockchain-based platforms marks a significant step towards a future where data integrity, transparency, and trust in digital environments are heightened. As blockchain technology continues to reshape various industries and redefine how we handle and exchange data, the preservation of the origin and security of that data is extremely important.

The combination of Chain of Custody with blockchain systems combines traditional evidence management principles with the advanced capabilities offered by distributed ledger technology. It establishes an unchangeable record-keeping mechanism that not only protects against manipulation but also ensures that every movement and transaction involving data cannot be challenged. This level of responsibility, supported by cryptographic principles, strengthens the credibility of blockchain networks.

Furthermore, the importance of maintaining a Chain of Custody goes beyond just ensuring data security and legal compliance. It also promotes a culture of transparency and accountability, which helps to build confidence among users, stakeholders, and organizations that rely on blockchain-based systems. Whether it is managing digital assets, conducting financial transactions, or verifying the authenticity of digital records, having a Chain of Custody in place provides assurance that data has been handled with utmost care and in accordance with established protocols.

In today's ever-changing landscape of digital assets, decentralized networks, and emerging technologies, understanding the significance of maintaining a Chain of Custody in blockchain-based systems is crucial. It emphasizes the commitment to upholding the highest standards when it comes to data integrity and trustworthiness within an increasingly complex and interconnected digital world.

In essence, the incorporation of Chain of Custody into blockchain-based systems represents a shift in how we handle and safeguard data rather than just its evolution. It sets the way for a

time when digital transactions are supported by blockchain technology's revolutionary potential and characterized by transparency, security, and uncompromising responsibility.

In conclusion, whether it means maintaining of physical or digital evidence, evidence management is an important aspect of the criminal justice system. It fulfills the vital functions of supporting the validity of the evidence, defending individual rights, and maintaining the fairness of court procedures.

In order to prevent contamination or tampering with physical evidence, meticulous protocols are required, and the chain of custody is crucial in monitoring each stage of the evidence's journey from the crime scene to the courtroom. In addition to helping the prosecution and defense, this increases public confidence in the fairness of the criminal justice system as a whole.

9. REFERENCES

[1] Sevenster M, Buurman J, Liu P, Peters JF, Chang PJ. Natural Language Processing Techniques for Extracting and Categorizing Finding Measurements in Narrative Radiology Reports. Appl Clin Inform. 2015;6(3):600-110. Published 2015 Sep 30.

[2] S.L., Berrahou & Buche, Patrice & Dibie-Barthélemy, Juliette & Roche, Mathieu. (2013). How to extract unit of measure in scientific documents?

[3] Hundman, K., & Mattmann, C. A. (2017). Measurement context extraction from text: Discovering opportunities and gaps in earth science. In arXiv [cs.IR].

10.GLOSSARY

- Natural language processing

- Recurrent Neural Network (RNN)

11.APPENDICES