BLOCKCHAIN BASED CRIMINAL INFORMATION MANAGEMENT SYSTEM IN SRI LANKA

TMP-23-270

Proposal Project Report

Thushitharan. M – IT19983370

B.Sc. (Hons) in Information Technology Specializing in Cyber Security

Department of Computer System and Engineering

Sri Lanka Institute of Information Technology Sri Lanka

March 2023

BLOCKCHAIN BASED CRIMINAL INFORMATION MANAGEMENT SYSTEM IN SRI LANKA

TMP-23-270

Proposal Project Report

Thushitharan. M – IT19983370

B.Sc. (Hons) in Information Technology Specializing in Cyber Security

Supervisor – Mr. Kanishka Yapa

Co-Supervisor – Ms. Dinithi Pandithage

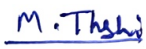
Department of Computer System and Engineering

Sri Lanka Institute of Information Technology Sri Lanka

March 2023

DECLARATION

I declare that this is our own work, and this proposal 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 our 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.

Name	Student ID	Signature
Thushitharan. M	IT19983370	

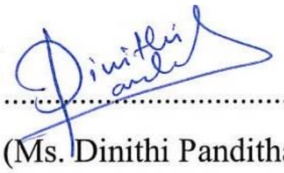
The above candidate is carrying out research for the undergraduate Dissertation undermy supervision.

Signature of the supervisor Date

..... 5/4/2023

(Mr. Kanishka Yapa)

Signature of the co-supervisor Date



..... 6/4/2023

(Ms. Dinithi Pandithage)

ABSTRACT

The crime rate in Sri Lanka has been increasing day by day. The criminal records management system in Sri Lanka has been facing challenges related to the integrity, accuracy, and accessibility of criminal records. These challenges can lead to inefficiencies in investigations, wrongful convictions, and a lack of accountability for criminal justice stakeholders. In order to address these challenges, this project proposes a blockchain-based chain of custody system for managing criminal records in Sri Lanka. The proposed system will use blockchain technology to create an immutable record of custody transfers for criminal records. This will ensure that custody of records is accurately and securely tracked, and that the chain of custody can be easily audited and verified. The system will also allow for secure and decentralized access to criminal records, reducing the risk of tampering and improving accessibility for criminal justice stakeholders. The project will be implemented through a collaboration between the Sri Lankan government and a blockchain development company. The project team will work closely with stakeholders in the criminal justice system to ensure that the system is designed to meet their needs and that it is compatible with existing systems and processes.

Key words – Blockchain, chain of custody, digital evidences, users, integrity

ACKNOWLEDGEMENT

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 FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

CRMS – Criminal Records Management System

CoC – Chain of Custody

IPFS – Inter Planetary File System

B-CoC – Blockchain-Chain of Custody

1 . INTRODUCTION

1.1 Background and Literature Review

Criminal activities are uncontrollable nowadays. They have been increasing day by day as a various kind of malicious activities. In this case Criminal Records Management System is mandatory for every country. Crime evidence management is one of the important parts in the Criminal Records management system. Managing evidence is a crucial issue in digital forensics. Digital evidence plays a critical role in crime investigations, as it is used to connect individuals to their criminal actions.

In digital forensics, chain of custody refers to the process of documenting and keeping a chronological history of handling digital evidence. This process is vital as it records all the relevant details of digital evidence at different levels of hierarchy, from the first responder to the higher authorities responsible for investigating cybercrime. Chain of Custody presents particular challenges in managing digital proof. The use of blockchain technology can facilitate transactions in various sections, providing significant advantages to the forensic community. In general, blockchain technology involves a decentralized and tamper-proof arrangement of blocks holding a cluster of individual transactions in a peer-to-peer network. It originally served the Bitcoin cryptocurrency as a fully replicated append-only ledger, and all nodes on the chain maintain a complete local copy of the blockchain. Each blockchain contains a hash of a previous block and a timestamp that tracks the creation and modification time of a document. Security-wise, nobody should be able to modify it once it has been recorded, and blockchain technology can prevent that (unless the integrity of time stamper is compromised, which is rare).

The blockchain technology was invented in 2008 and was implemented in 2009 to function in the general public dealings' ledger of the cryptocurrency bitcoin. Blockchain technology is decentralized, implemented in a world network of computers that records each bitcoin dealing managed by its network. The blockchain technology architecture shown in Figure 1 implements a decentralized, fully replicated append-only ledger in a peer-to-peer network, originally employed for the bitcoin cryptocurrency.

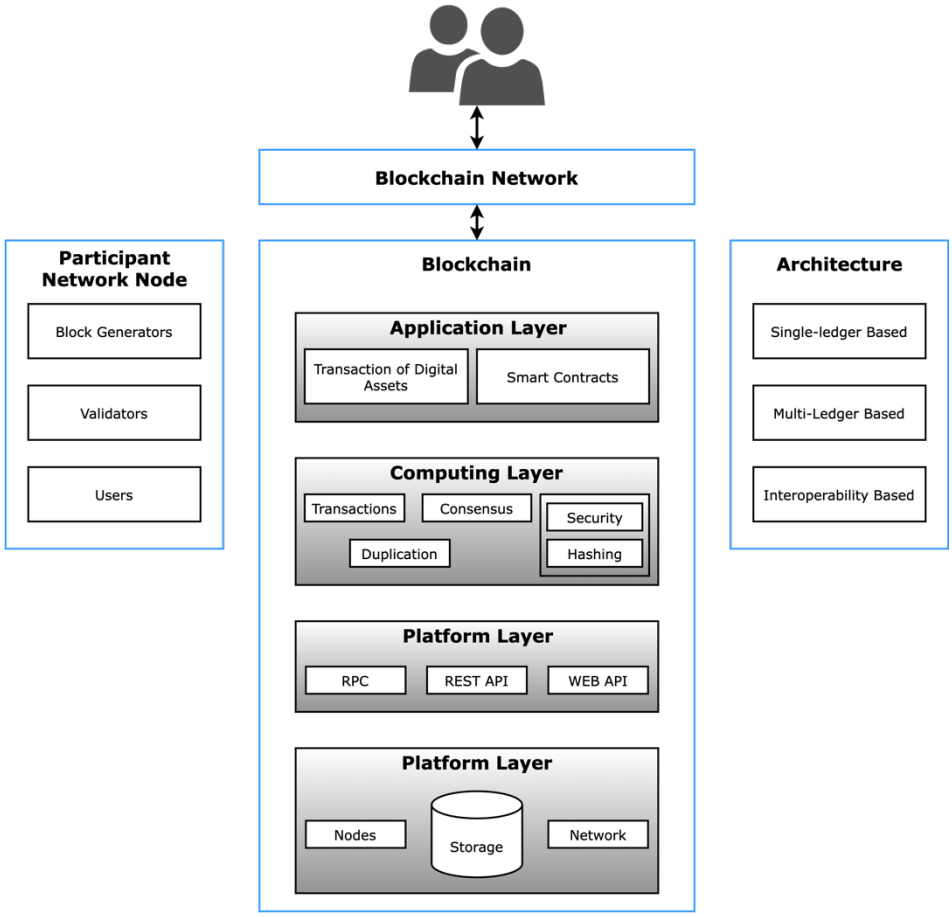


Figure 1: Overview of Blockchain Technology Architecture

1.2 Research Gap

Before the emergence of blockchain technology, traditional evidence management involved the use of paper-based documentation, spreadsheets, or databases to track the movement and custody of evidence. This process required human intervention and was prone to errors, tampering, and loss. Evidence would be collected and packaged with a physical paper evidence tag that would be manually filled out and signed by the officer who collected the evidence. This tag would then be transferred along with the evidence to the property and evidence room where the evidence would be logged into a computer system and assigned an item number. The officer would then be responsible for tracking the evidence through the system and providing updates on its status. Any changes in custody or location would be recorded in the system and the physical evidence tag would be updated accordingly. This process was time-consuming, inefficient, lack of integrity and had limited transparency.

Lack of a safe and impenetrable method to maintain digital evidence is where research is lacking in building a blockchain-based chain of custody evidence management system. Even

though law enforcement agencies have used traditional methods of evidence management, they are susceptible to manipulation and unauthorized access. These outdated procedures lack openness and accountability, which makes it difficult to establish the reliability of digital evidence in court.

Additionally, the complexity and volume of digital data are growing, making the current tools and techniques for digital forensics insufficient to handle them. Blockchain technology has the potential to address the constraints of current digital forensic procedures when it comes to dealing with dispersed systems and networks.

Table 1: Comparison of major functionalities about traditional system and our proposed system

	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

Process: Traditional evidence management often relies on manual processes, which can be time-consuming and prone to errors. For instance, evidence might be misplaced, mislabeled, or mishandled, leading to inaccurate or incomplete records. But the proposed system digitalizes all the process from evidence collection and preservation of them.

Security: Traditional evidence management systems may be vulnerable to security risks, such as theft or tampering. Without adequate security measures in place, evidence may be compromised or even destroyed. Blockchain technology ensures the security of digital evidence by providing tamper-proof records that are highly secure

Transparency: Traditional evidence management systems may lack transparency, which

can undermine trust in the criminal justice system. Without clear records and a standardized process, it can be difficult to ensure that evidence is being handled properly and fairly. But the Blockchain technology provides transparency in the chain of custody process by providing a publicly accessible, decentralized ledger that can be accessed by authorized parties.

Immutability: Traditional evidence management systems can be mutable. But in blockchain based systems, once a transaction is recorded on the blockchain, it cannot be altered or deleted, providing an immutable record of the chain of custody.

Efficiency: Blockchain-based evidence management can automate many of the manual processes involved in traditional evidence management, leading to increased efficiency and reduced costs.

1.3 Research Problem

The research problem addressed in the development of a blockchain-based chain of custody evidence management system is the need for a more secure and transparent method of handling and preserving digital evidence. Traditional methods of evidence management have been known to have flaws in the chain of custody, which can result in legal challenges that could hinder successful prosecution. Furthermore, the increase in the use of digital evidence in investigations has made it more challenging to manage the evidence in a secure and reliable manner.

The investigation of a crime is reliant on both physical and digital evidence. The justice system has become increasingly adaptable in accepting digital evidence since the handling procedure is comparable to that of physical evidence. As the digital investigation field continues to expand, it necessitates skilled computer investigators who can gather evidence from the crime scene, retrieve call data records, examine collected information, recover lost data, and participate in the forensic process.

"In order for qualified forensic science experts to testify competently about forensic evidence, they must first find the evidence in a usable state and properly preserve it."

- National Academy of Sciences, *Strengthening Forensic Science in the United States: A Path Forward* (2009)

2. RESEARCH OBJECTIVE

2.1 Main Objective

The main objective of a research project on blockchain-based chain of custody evidence management could be to evaluate the effectiveness and feasibility of implementing blockchain technology in the evidence management process, with a focus on enhancing security, integrity, and transparency in the handling of digital evidence, while reducing the risk of tampering or corruption. The study could aim to assess the benefits and limitations of blockchain-based chain of custody evidence management, such as its impact on reducing the time and cost of investigations, improving collaboration and information sharing among stakeholders, and enhancing trust and accountability in the justice system. the cost of implementation, and the potential legal and ethical implications. Overall, the objective of the research project would be to contribute to the development of more efficient and effective methods for managing digital evidence in criminal investigations.

2.2 Specific Objective

In order to achieve the main objective, following specific objectives have to be accomplished,

1. Investigate the current challenges faced by law enforcement agencies in managing digital evidence and analyze how a blockchain-based solution can mitigate these challenges.
2. 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.
3. 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.
4. 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.
5. Examine the legal and ethical implications of using blockchain technology in evidence management, including issues related to privacy, confidentiality, and admissibility in court.

6. Propose guidelines and best practices for the use of blockchain-based chain of custody evidence management systems in law enforcement agencies.

3. METHODOLOGY

The proposed system will have to consists of the following methodologies to achieve the goals of the research. This methodology provides a general framework for implementing a blockchain-based chain of custody evidence management system, but the specific steps and processes may vary depending on the organization's needs and the chosen blockchain platform. This method's primary phase is to derive concepts from knowledge base data and then apply the deductive process to create a relationship between the model's key variables. The overall procedure emphasizes a continuous dialogue between the phases of inductive data and analysis. Ultimately, this leads to the development of a sound analysis of the potential and applicability of blockchain and smart contracts to enhance Chain of Custody and the model for handling digital evidence. Additionally, fundamental metrics are taken into account to enhance traceability and evidence sources, such as evidence:

- 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

More than this, there are some additional methodologies listed here to develop out proposed system.

- **Identify the requirements**: Define the system requirements based on the needs of the stakeholders and the goals of the organization.
- **Design the user interface**: Create a user-friendly interface that allows authorized users to interact with the system and perform necessary actions, such as adding or retrieving evidence.
- **Integrate with existing systems**: Integrate the blockchain-based chain of custody system with other relevant systems, such as forensic tools or case management software.
- **Train users**: Train all relevant users, including investigators, administrators, and IT staff, on how to use the new system effectively and securely.
- **Test and deploy**: Conduct thorough testing to ensure the system is functioning as

expected and that the evidence is secure. Deploy the system and monitor its usage to identify any potential issues or improvements.

- **Maintain and update**: Regularly maintain and update the system to ensure it remains secure and meets the changing needs of the organization.

3.1 System Architecture

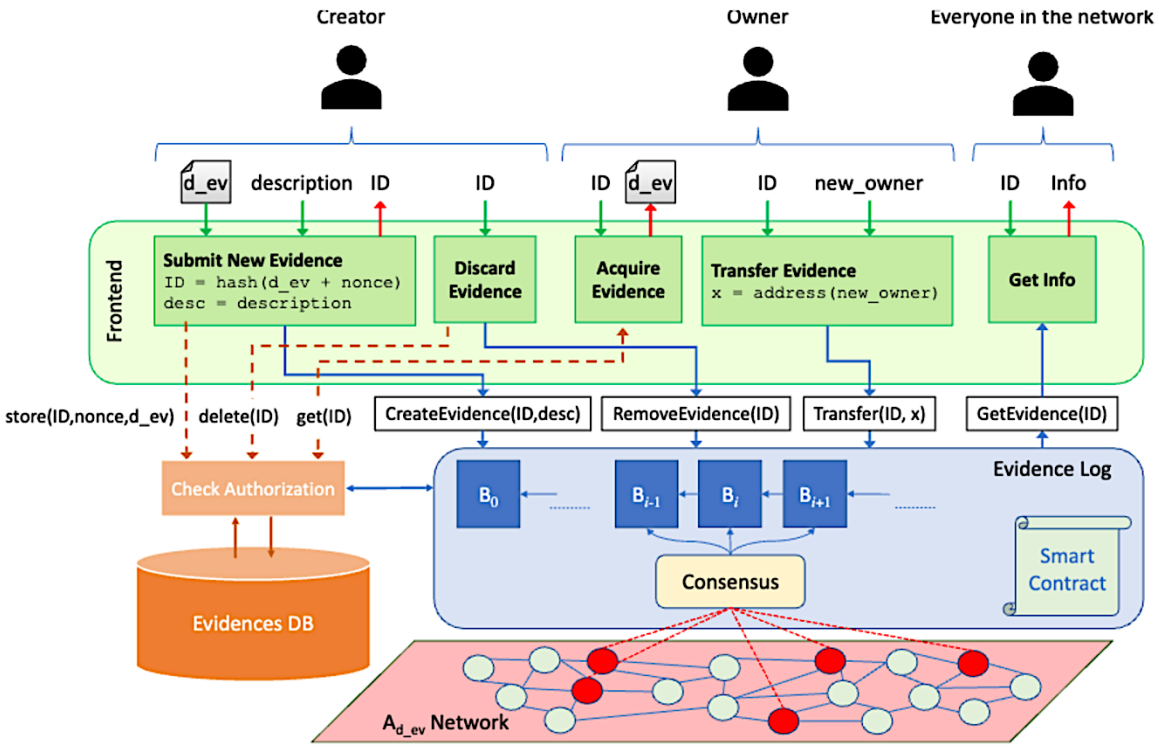


Figure 2: Blockchain Chain of Custody Architecture

This image proposes the base overview architecture of Blockchain-based Chain of Custody, which is built on a private, permissioned blockchain. This decision was made in response to the CoC process's authentication requirement, which forbids unauthorized and untrusted parties from managing digital evidence and, as a result, from participating in the network.

The Evidence DB, the Evidence Log, and the Frontend interface make up the majority of B-CoC, as depicted in Figure 1. The actual digital evidence is kept in the Evidence DB, a standard database and/or file repository, while information about the CoC is kept in the Evidence Log, a blockchain-based application. There are two reasons for this division. First off, some evidence may be too big to be stored efficiently on the blockchain (evidence may be, for instance, a bit-by-bit copy of a storage device with several TBs of capacity). Second, and most critically, storing evidence in the blockchain would give every node in the network access to them, whereas only authorized nodes should be able to obtain evidence. Therefore, we only store information about the CoC process and a hash of the evidence that allows for verification in the blockchain.

Evidence DB: The original digital evidence is saved in the Evidence DB, a regular database and/or

file repository, together with an ID obtained from the hash of the evidence and a nonce (to ensure IDs are unique). This database is disseminated and administered by reputable organizations, like law enforcement personnel in courts. Additionally, each access is only carried out if the requesting organization has the necessary authorization for it based on its function.

Evidence Log: The Evidence Log uses blockchain technology to keep information about each piece of evidence, including its ID, a description, the identity of the submitter (also known as the originator), and the whole history of previous owners, up to and including the present owner. Although the evidence itself is not stored in the blockchain, it is important to note that, provided a strong cryptographic hash function is used to generate it, the ID allows to verify that the evidence has not been tampered with. The implementation of the evidence log sits on top of a peer-to-peer network made up of all authorized entities. A network like this can be divided into two sets of nodes:

- **Validator nodes:** Mostly perform the following functions: Keeping a copy of the blockchain, confirming transactions, and creating, proposing, and adding blocks to the chain are all examples of ways to participate in the consensus protocol.
  This group of nodes is required to be preventively allowed in the permissioned blockchain in order to serve as validators.
- **Lightweight nodes**: Since they just issue transactions and depend on validators to add and validate them, they can be thought of as clients of the chain.

3.2.1 Technologies used in this system.

Table 2: Technologies that are going to be used in this project.

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

3.2.2 Software Specification

- The Blockchain Based Criminal Records Management system requires component by component software development. As Chain of Custody Evidence Management is my component, It needs a faster development, So I planned to continue the development process using Agile software development process.

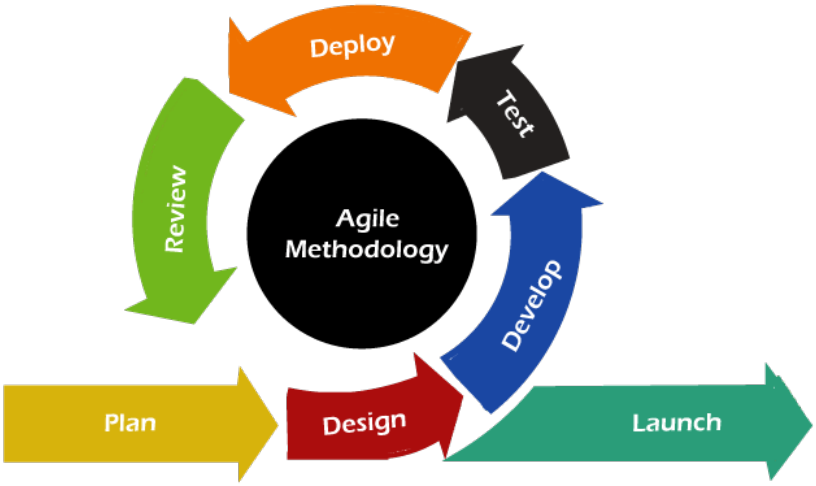
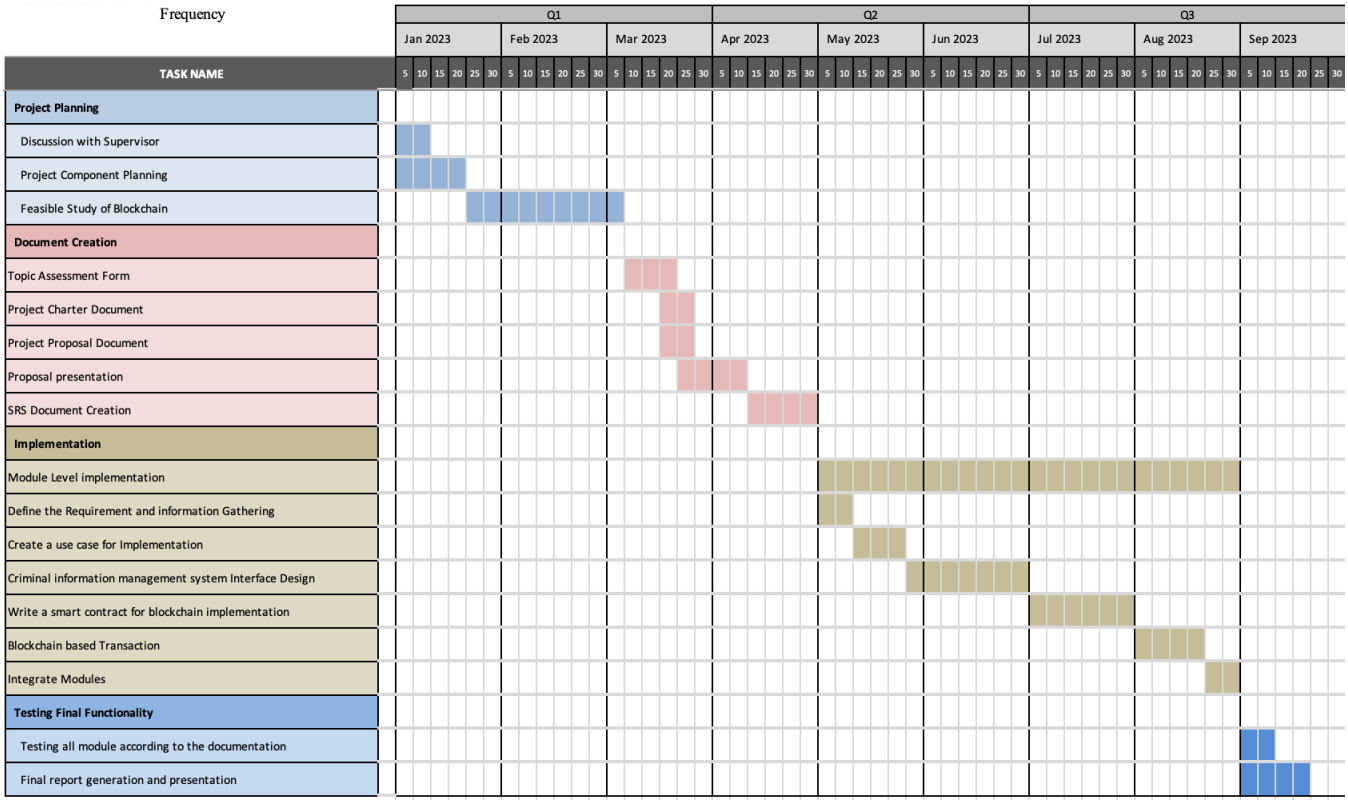


Figure 3: Agile Process

- **Planning**: This step involves defining the product vision, scope, goals, and priorities. The product owner and the development team can work together to plan the project and set timelines for each iteration.
- **Requirements Analysis**: The development team and product owner can work together to identify the necessary features and requirements for the system.
- **Design**: The development team can design the system architecture and user interface to meet the requirements.
- **Development**: The development team can work on creating the blockchain-based system and the chain of custody evidence management features in iterative sprints.
- **Testing**: The development team can test the system at each iteration to ensure the system is functioning as expected.
- **Delivery**: After each sprint, the team can deliver a functional version of the system to the stakeholders for review and feedback.
- **Deployment**: Once the system is fully developed, it can be deployed to the target environment and made available to the end-users.

4. GANTT CHART



5. BUDGET

The total budget for the proposed component.

Component	Amount (USD)	Amount (LKR)
Cloud Server Cost	10$	3200
Third Party API Costs	15$	4800
Internet Cost	15.62 $	5000
Total cost	**40.62$**	**13000**

6. COMMERCIALIZATION

The market value is very low this product. Because this system should be used by authorized authors confidential. The proposed system is mainly targeted to Department of Police and Law firm. The main actors who are going to use this system are police investigators and lawyers. Police investigators can use this system to add, verify, check-in, review, check-out the digitalized evidence. Lawyers can use this system to get the copy of the evidence to the respective cases.

The system can improve the accuracy and reliability of criminal records, making it easier for law enforcement to investigate and prosecute crimes. The system can also streamline the process of sharing criminal records between agencies and jurisdictions, saving time, and reducing errors. Additionally, the immutable nature of blockchain technology can help prevent tampering or falsification of records, ensuring their integrity. Lawyers can benefit from the system as well, by having access to a more comprehensive and accurate set of criminal records to inform their legal strategies. Overall, the system can improve the efficiency and effectiveness of the criminal justice system for both law enforcement and legal professionals.

7. REFERENCE LIST

[1] Prayudi, Yudi & Sn, Azhari. (2015). Digital Chain of Custody: State of The Art. International Journal of Computer Applications. 114. 975-8887. 10.5120/19971-1856.

[2] Anderson, G.S., Litzenberger, R. and Plecas, D. (2002), "Physical evidence of police officer stress", Policing: An International Journal, Vol. 25 No. 2, pp. 399-420.

[3] Tasnim, Maisha & Omar, Abdullah & Rahman, Shahriar & Bhuiyan, Md. (2018). CRAB: Blockchain Based Criminal Record Management System. 294-303. 10.1007/978-3-030-05345-1_25.

[4] S. D. A. S. K. T. R. S. S. A. Jain, "Blockchain-Based Criminal Record Database Management," in 2021 Asian Conference on Innovation in Technology (ASIANCON), PUNE, India, 2021

[5] Robert Lentell (2000) Untangling the tangibles: 'physical evidence' and customer satisfaction in local authority leisure centres, Managing Leisure, 5:1, 1-16, DOI: 10.1080/136067100375704

[6] Ćosić, Jasmin & Ćosić, Zoran. (2012). Chain of custody and life cycle of digital evidence. Journal of computer technology and application.

[7] Alruwaili, Fahad. (2021). CustodyBlock: A Distributed Chain of Custody Evidence Framework. Information. 12. 88. 10.3390/info12020088.

[8] Ali, Mohamed & Ismail, Ahmed & Elgohary, Hany & Darwish, Saad & Mesbah, Saleh. (2022). A Procedure for Tracing Chain of Custody in Digital Image Forensics: A Paradigm Based on Grey Hash and Blockchain. Symmetry. 14. 334. 10.3390/sym14020334.

[9] Barbara Guttman, Douglas R. White, and Tracy Walraven; Digital evidence preservation: considerations for evidence handlers.

[10] Williams, S. , Taylor, M. , Ballou, S. , Stolorow, M. , Kline, M. , Bamberger, P. , , L. , Brown, R. , Yvette, B. , Dennis, D. , DePalma, L. , Hunt, T. , , C. , Keaton, R. , Kiley, W. , Latta, J. , Thiessen, K. , LaPorte, G. , Ledray, L. , Nagy, R. , Ostrom,

B. , Schwind, L. and Stoiloff, S. (2015), Biological Evidence Preservation: Considerations for Policy Makers, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.IR.8048 (Accessed May 8, 2023)

[11] Ballou, S. , Kline, M. , Stolorow, M. , Taylor, M. , Williams, S. , Bamberger, P. , Yvette, B. , Brown, L. , Jones, C. , Keaton, R. , Kiley, W. , Thiessen, K. , LaPorte, G. , Latta, J. , Ledray, L. , Nagy, R. , Schwind, L. , Stoiloff, S. and Ostrom, B. (2013), The Biological Evidence Preservation Handbook: Best Practices for Evidence Handlers, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.IR.7928 (Accessed May 8, 2023)