

BLOCKCHAIN BASED CRIMINAL INFORMATION MANAGEMENT SYSTEM IN SRILINKA

TMP-23-270

Proposal Project Report

Brahanawardhan B – IT20150952

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 SRILINKA

TMP-23-270

Proposal Project Report

Brahanawardhan B – IT20150952

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

We 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 |
|------------------|------------|-----------------------|
| Brahanawardhan B | IT20150952 | <i>brahanawardhan</i> |

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

Signature of the supervisor

Date

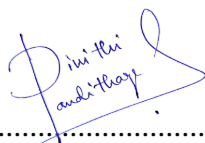


03/04/2023

.....
(Mr. Kanishka Yapa)

Signature of the co-supervisor

Date



03/04/2023

.....
(Ms. Dinithi Pandithage)

ABSTRACT

Due to the current economic crisis in Sri Lanka, people's lifestyle in difficult conditions. Due to this, crimes are increasing rapidly. The graph of criminal activities steadily increasing the country because of an economic crisis and the Globalization of ultra-modern technology. In many industries today, blockchain applications are being explored as a secure and cost-effective method to manage a distributed database and keep track of all types of digital transactions. In Sri Lanka the existing criminal information management system is traditional approach like paper basis. Storing, retrieving, updating the criminal records are highly time consuming. As results, it causes many drawbacks. To address the drawback our team is proposing Blockchain based technology for criminal information management system called “CRISYS”. Blockchain can take the position of the accumulation of criminal records with a network where criminal records information is easily accessible within the organization, secure, and it cannot be altered. A P2P (peer-to-peer) network called blockchain aids in the decentralization of criminal Records, as a result, to maintain a ledger to prevent a single point of failure (SPOF), and all the criminal records will be updated and validated in real-time. Because they are easily accessible and unbreakable, decentralized networks with straightforward algorithms are safe and cryptographically secured. Blockchain's peer-to-peer network facilitates the sharing of information within organizations. To ensure criminal records' confidentiality and integrity, this system will be built on the immutability feature of blockchain. By developing this blockchain-based system, the corruption of risk factors can be reduced. allowing greater objectivity and consistency and improving the transparency and accountability of criminal records. Real access at the right time to Criminal histories with appropriate administrative agencies to improve policy and law enforcement effective.

Keywords – Blockchain, Security, Criminal Records, decentralization, smart contracts

ACKNOWLEDGEMENT

I Place on record and warmly acknowledge the continuous encouragement, invaluable supervision, timely suggestion, and inspired guidance offered by our guide Mr. Kanishka Yapa, Supervisor, and Ms. Dinithi Pandithage, Co-Supervisor, and Research project team. We would like to express our sincere thanks to everyone who contributed to this research project. First and foremost, we would like to thank our supervisors for their guidance and support throughout the research process. Their valuable insights and feedback were instrumental in shaping the direction of this proposal.

TABLE OF CONTENTS

| | |
|--|----|
| DECLARATION | 1 |
| ABSTRACT | 2 |
| ACKNOWLEDGEMENT | 3 |
| TABLE OF CONTENTS | 4 |
| LIST OF TABLES | 5 |
| LIST OF FIGURES | 6 |
| 1 INTRODUCTION | 7 |
| 1.1 Research Background | 7 |
| 1.2. Literature Survey | 8 |
| 1.2.1. Implementing Smart contract in blockchain | 8 |
| 1.3. Research Gap | 11 |
| 1.1 Research Problem | 13 |
| 2. OBJECTIVE | 14 |
| 2.1 Main Objective | 14 |
| 2.2 Specific Objective | 14 |
| 3. Research Methodology | 17 |
| 3.1. Step for Implementation | 18 |
| 3.2. High Level Architecture | 19 |
| 3.3. Major Components | 20 |
| 3.2.1. Blockchain System | 20 |
| 3.4. Technologies used in the project. | 21 |
| 3.5. Gantt Chart | 24 |
| 4. BUDGET | 25 |
| 5. Commercialization | 26 |
| 6. Reference List | 27 |

LIST OF TABLES

Table 1.1 Tabularized format of Research Gap.....12

Table 1.2 Research Project Timeline.....24

Table 1.3 Research Budget.....25

LIST OF FIGURES

| | |
|---|----|
| Figure 1: A Block | 08 |
| Figure 2: Hash in a block..... | 08 |
| Figure 3: Increasing rates of criminal records in Sri Lanka..... | 13 |
| Figure 4: High level of criminal Information Management System..... | 19 |
| Figure 5: Commercialization Product..... | 26 |

1 INTRODUCTION

1.1 Research Background

Criminal Information management is a vital component of any effective criminal justice system. Crimes in our daily life are increasing to an uncountable level due to the current economic crisis in our country the daily life of the people is in a difficult situation due to which allegation activities like theft, money laundering, bribery and extortion are happening daily in our country due to which people are becoming criminals and police stations in our country are acting dishonestly. Accusations are being covered up as they come. Apart from that there is an increase in the number of records of criminals in police stations due to which police departments have massive problems in handling records of criminals and witness documents. As far as our country is concerned, the complaint handling system is maintained manually and on a small computer basis. Due to this there are many drawbacks and defects in the system, such as limited amount of accessibility, a lack of transparency, and concerns about critical data Security and the integrity of criminal records. This has made it challenging for law enforcement organizations to share information across various platforms and to monitor and manage criminal proceedings effectively.

A potential remedy for these drawbacks is blockchain technology. Therefore, our team is going to proposed “Blockchain based Criminal Information Management System” (CRISYS) to address the problem. Blockchain is a decentralized, decentralized database that allows for secure, accessible, and immutable transactions between organizations. A blockchain-based criminal information management system could provide improved security and transparency within a decentralized network, as well as increased efficiency in tracking and handling criminal cases, by utilizing the advantages of blockchain.

However, research on the subject is limited, especially in the Sri Lankan context, and the use of blockchain technology in criminal information management is still in its infancy. In the context of the benefits, challenges, and feasibility of a blockchain-based criminal information management system in Sri Lanka, this research aims to investigate its potential.

1.2. Literature Survey

1.2.1. Implementing Smart contract in blockchain

For a criminal information management system, blockchain technology plays a major role as per the research objective. Because of that our team has to provide an effective and efficient Blockchain based Crime Information Management System to the Police Department in Sri Lanka. When we think about the crime information management environment in Sri Lanka, different types of users (police, lawyers, administration, public) can use our system. But the most noted point is these users are categorized in role based and rule based because particular user can access the restricted information only. Therefore, we are implementing Access control for our proposed system. The blockchain technology introduced for criminal records management to address our existing problem.

[1]

Aastha Jain, Soumyajit Das, Anand Singh Kushwah, Tushar Rajora, Shagun Saboo
"Blockchain based criminal Record Database Management."

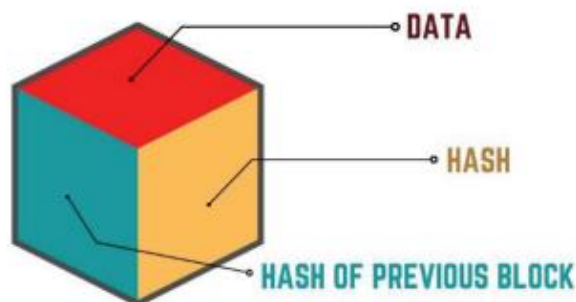


Figure 1: A Block [2]

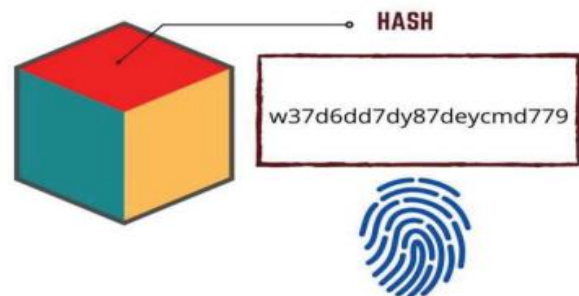


Figure 2: Hash in a Block [2]

(Figure 1) Any type of data could be stored in the block. All the criminal records will be kept in this block. It contains a unique value called a hash, which once verified acts like a fingerprint that is accessible across all network peers. Each block [2]

- Contains Hash value of the block.
- Cryptographic hash of the previous block.
- The time in seconds since 1970-01-01 T00:00 UTC.
- The goal of the current difficulty.
- The root hash of Merkle tree

It also contains the hash value of the previous block to create a chain of blocks containing the records. As new record entered, it creates a new block. Once the block is populated with records, it is merged with the previous block, putting the data together sequentially.

(Figure 2) Hash is a Mathematical operation can be converting an input of arbitrary length into an encrypted output of a fixed length. As a result, its unique hash value is always the same size, independent of the original data or file size.

On the other side, hashing is a one-way function that cannot be decrypted back to original data. A system based on the SHA-256 mathematical algorithm (Secure hashing algorithm - 256). This methodology will prevent from the unauthorized access and confidentiality, Integrity, and Availability violation. To review this research paper, I understand the point of How blockchain based Application works.

Cho, K. H., & Lee, C. (2020). Blockchain-based criminal records management system. In 2020 IEEE International Conference on Big Data and Smart Computing (BigComp) (pp. 480-485). IEEE.

Several research studies have explored the potential of the blockchain technology in criminal justice. For example, Cho and Lee (2020) developed a blockchain based criminal records management system and demonstrated its feasibility through a proof-of-concept prototype. Their system uses the decentralized and tamper-proof nature of blockchain to improve the security and transparency of criminal records management.

Kshetri, N. (2018). Can blockchain strengthen the internet of things? IT professional, 20(4), 68-72.

Other researchers have also proposed various blockchain-based strategies to improve the criminal justice system. A blockchain-based network was developed by Wust et al. (2018) to store and share forensic evidence, which would improve its discoverability and integrity. Meanwhile, Kshetri (2018) suggested using blockchain technology to confirm the identification of criminal suspects, which could reduce the possibility of wrongful arrests and increase the effectiveness of criminal investigations.

Maras, M. H., & Greenfield, V. A. (2018). Blockchain technology: Implications for data privacy and security in criminal justice. Journal of Criminal Justice Education, 29(3), 369-382.

Further research points out the possible privacy and security advantages of blockchain-based criminal information management systems. Blockchain technology, for instance, has been proposed as a potential solution to the issue of data breaches and illegal access to private criminal records by Maras and Greenfield (2018). They proposed a system based on blockchain technology that would provide people more control over their private information while enabling authorized parties to access the data they require for legal reasons.

1.3. Research Gap

As mentioned above, during the literature review we have found there are similar Criminal Information Management systems which have been already created using blockchain concept, according to our analysis In Sri Lanka criminal Information Management system all operation will based on the Manual Basis like hand filled forms and the printed Paper copies. And Some of the Higher police department in srilanka have a Centralized Criminal Information Management System. Due to this, there are several drawbacks in those criminal Information management systems. Due to the current economic crisis in Sri Lanka, police departments are facing a huge problem due to the increasing crime rate. Existing Criminal information Management Systems Includes massive amount of criminal Records that have in big ledgers in order to perform some action and stored the criminal records in small centralized databases. It will cause significant problems. Such as Interoperability problem when identifying criminals in criminal information management system, Lack of consistency when identifying Criminals, Lack of standards for sending, receiving, and managing information between criminal record management system and the lack of shared data in criminal record management system. To fill this problem I am going to proposed to use implementing blockchain-based smart contracts for Criminal information management system to get around this problem. For the Blockchain based Criminal system is to process the evidence and records with great security and efficiency. In our system, criminal records and forensic evidences will be stored and transferred using the Interplanetary File System (IPFS), which also uses a distributed file transmission protocol with a blockchain as its foundation. This IPFS system very helpful when we need to move info efficiently across a network.

In my research on implementing Blockchain based smart contract for Criminal Information Management system in Sri Lanka police departments. When I refer to the existing blockchain based technology, criminal Information Management System needs to consider. Implementing the smart contract between the criminal Information management and the blockchain technology. Smart contracts help to get response from

blockchain in very efficient manner. Our System will distribute the live/periodical update of the criminal Records within the decentralized networks. With our proposed solution the existing drawbacks are minimized.

Table 1.1 Tabularized format of Research Gap

| Consideration On | Existing Criminal Information Management System in Sri Lanka. | Blockchain Based Criminal Information Management System (Our Approach) |
|--|---|--|
| Security of Sensitive Criminal Records | LOW | HIGH |
| Decentralization Of System | LOW | HIGH |
| Ensure data Integrity | LOW | HIGH |
| Prevent loss of data | LOW | HIGH |
| Availability | LOW | HIGH |
| Confidentiality | LOW | HIGH |

The proposed solution consists of many Security functionalities when compared to existing research projects. The proposed solution will suggest different methods such as Immutable Criminal Records, Decentralization, Encryption, Smart contracts, Public/private key Infrastructure. As these results to ensure confidentiality, Integrity, and availability.

1.1 Research Problem

As the number of crimes is increasing day by day, there is a need for a more efficient and secure system to manage crime related information. According to our analysis, every police department in our country is facing a huge problem in dealing with ongoing allegations and related documents and records. Police Departments maintain criminal information records on a paper basis and through a small centralized system. One of the major challenges facing the current criminal information management system in our country is the security of information storage and the transparency, lack of security and immutability of criminal records in the system. These lead to numerous data breaches and unauthorized data changes, which have a significant and massive impact on individuals, organizations, and the government. Blockchain technology exists. Capable of providing a secure and transparent solution for criminal records management. A blockchain-based criminal information management system can use decentralized ledgers to store crime-related document records, thus ensuring that criminal information is stored securely and documents are undamaged. [4] The system therefore automates the process of using smart contracts, updating and accessing information, reducing the potential for human error.

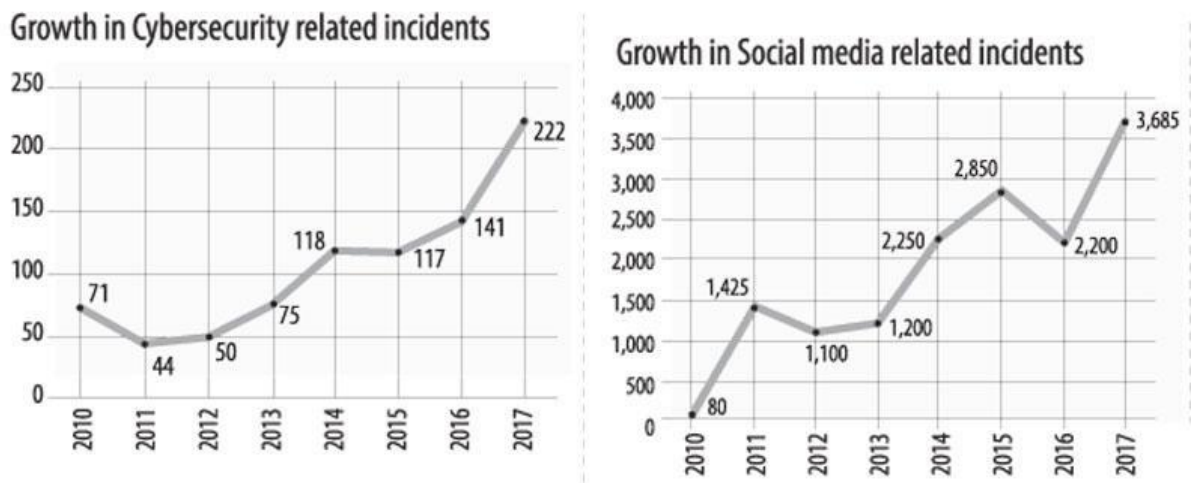


Figure 3: Increasing rates of criminal records in Sri Lanka.

2. OBJECTIVE

2.1 Main Objective

A blockchain-based criminal records management system's main objective is to provide a secure, accessible, and immutable platform for storing and managing criminal records. The use of blockchain technology can ensure that the records are stored in a decentralized and distributed manner, which makes them more secure and resistant to tampering or unauthorized modification. Additionally, a blockchain-based system to organize criminal data can aid in enhancing the effectiveness of the criminal justice system. Law enforcement agencies, courts, and other relevant organizations can quickly and easily access the information they need to make informed decisions by having all criminal records kept in a centralized and accessible platform.

2.2 Specific Objective

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

- **User Secure Data Management:** Managing criminal records securely and dependably is one of the main sub-objectives of a blockchain-based criminal information management system. This entails safeguarding the integrity of data, preventing data falsification, and preventing entry by unauthorized parties.
- **Efficient Data Sharing:** Facilitating successful information sharing among various criminal justice organizations and other authorized parties could be another sub-objective. To ensure that data is shared only with authorized parties, would necessitate the use of smart contracts, secure communication channels, and suitable access controls.

- **Ensuring Confidentiality, Integrity, and Availability:**

Maintaining the security and reliability of a blockchain-based criminal information management system depends on ensuring its confidentiality, integrity, and availability (CIA). Sensitive criminal data should be encrypted to ensure confidentiality, and only authorized personnel should be able to access it. Data stored in the blockchain should be immutable and protected from unauthorized modifications in order to ensure integrity. The system should be designed with redundancy and fault tolerance in mind to ensure availability.

- **Improved Case Management:** One potential use of a criminal information management system based on blockchain technology is to enhance the handling of criminal cases by allowing instant access to pertinent information like arrest records, past criminal activities, and case details. By doing so, it could facilitate the process of investigations and enable law enforcement agencies to apprehend suspects more efficiently.
- **Automated Workflow:** The criminal justice system's efficiency could be improved through automation, which could be a secondary goal of the system. This could involve automated procedures like identity verification, authorization, and data retrieval that can ease the burden on law enforcement officers and allow them to focus on other critical responsibilities.
- **Enhanced Transparency:** By making criminal data more accessible and traceable, a criminal information management system based on blockchain technology could offer increased transparency. This transparency could help foster accountability and lower the likelihood of corruption or misuse of authority.

- **Cross-border collaboration:** Enabling cross-border cooperation among diverse law enforcement agencies to enhance information sharing and coordinated action could be another goal of the system. Using a blockchain-based platform for international collaboration could offer a secure and dependable framework, improving worldwide law enforcement endeavors.
- **Awareness for Law Enforcement Agencies:** Law enforcement agencies need to be aware of the laws and regulations that apply to their jurisdiction. This includes criminal law, civil law, and other regulations that affect their operations. Law enforcement agencies must be aware of public safety issues that affect their community. This includes identifying and responding to potential threats to public safety, such as terrorism, natural disasters, and violent crime. Law enforcement agencies need to be aware of the latest technology that can assist them in their duties. This includes communication systems, surveillance equipment, and forensic tools. Law enforcement agencies must be aware of the communities they serve and work to build positive relationships with them. This includes understanding the concerns and needs of the community and engaging in outreach efforts. Law enforcement agencies need to be aware of cultural differences and how they may impact interactions with members of the community. This includes understanding cultural norms, language barriers, and the unique challenges faced by different groups.

3. Research Methodology

“CRISYS” (Blockchain Based criminal Information Management System) will be consisting of the following major modules:

- Blockchain System for Criminal Records
- Smart Contract with Encryption
- Ganache Personal Blockchain
- Truffle Framework
- MetaMask Ethereum Wallet
- Criminal Information Management System Interface

The objective of this paper is to propose the concept of a more robust and secure system for storing all criminal records. In this section, we will elaborate on the architecture of our system. Our approach is centered on a decentralized and distributed network that utilizes a technique to link all blocks into a chain for storing criminal data. Assume there are four steps in the process to better understand it. [4]

- **The Admin Officer:** Once the Admin officer receives information about a crime, they enter the data into the system, which generates a block and eliminates the need for paperwork.
- **Validation Of Data:** Once a block has been generated on the network, a copy is distributed to all network peers for verification and validation. If a block has been tampered with in any way within one peer network, it will not be authenticated by the rest of the network members. As a result, only verified data will be present on the network.

- **Availability of criminal data across the peer-to-peer network:** Once the data has been validated by the miners, it is stored permanently on every blockchain node. Since the data is stored immutably, it is considered verified and authenticated, which allows people to access the data from anywhere with ease.
- **Access Data:** Authorized individuals can access the data using a unique case ID and the associated hash.

3.1. Step for Implementation

1. **Determine the Problem** – In Sri Lanka Police department are depending on local database and paper basis system to address this issues implement smart contract with the Encryption for Criminal Information Management System.
2. **Choose a blockchain platform** – Ethereum blockchain platform for implementing decentralized network for our proposed system.
3. **Define the smart contract** – Define the rules and logic and behavior of blockchain based smart contract for the criminal system. Which includes specifying the inputs, outputs, and state variable of the contract.
4. **Write the smart contract code** – Use a solidity programing language supported by Ethereum blockchain platform to write the code for smart contract.
5. **Test the smart contract** – use testing framework and tools to test the functionality and security of smart contract. This includes unit testing, integration testing and security testing.
6. **Deploy the smart contract** – Deploy the smart contract for Ethereum blockchain platform using the appropriate deployment tools and processes. verify the correctness of the deployment and record the contract's address.

7. Interact with the smart contract.
8. Monitor and maintain smart contracts.

3.2. High Level Architecture

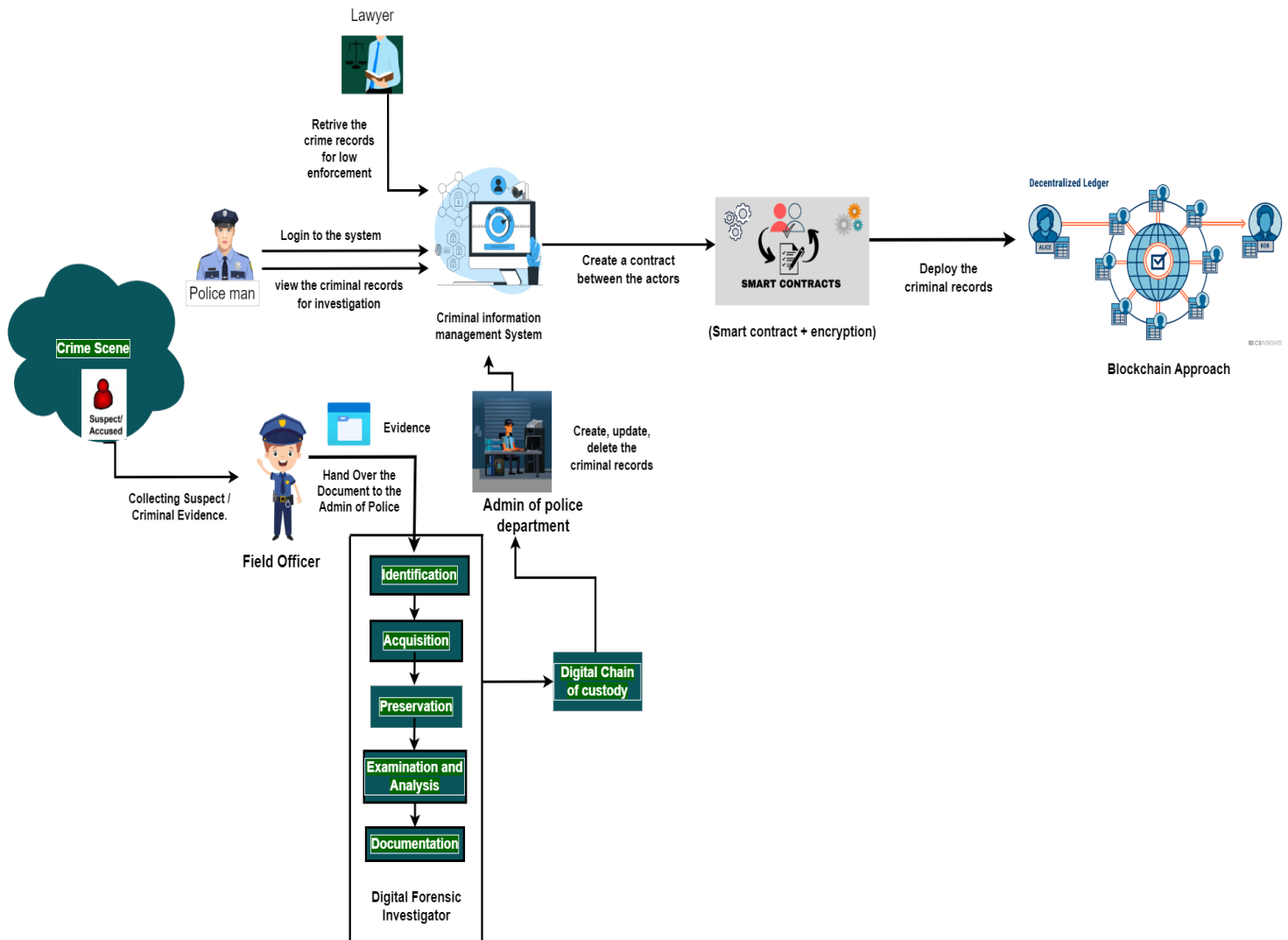


Figure 4: High level of criminal Information Management System

3.3. Major Components

3.2.1. Blockchain System

Criminal Information Management

In order to develop a blockchain system for criminal information management, several important steps need to be taken. First, a decentralized network of nodes must be built that work together to maintain the integrity of the blockchain. Next, smart contracts need to be defined to govern how criminal information is added to the blockchain. These contracts may require criminal information to be reviewed by multiple law enforcement agencies before it can be added. The blockchain's data structure must also be designed to accommodate criminal information, with each record represented by a unique hash containing relevant information about the person.[5] Maintaining the security and integrity of the system requires user roles and permissions to be set up, with law enforcement allowed to add criminal information and members of the public with read-only access. Finally, the system must be secured through encryption, multi-factor authentication, and regular system checks to prevent unauthorized access and ensure data integrity.

Nodes and Miner Nodes

A Criminal Information Management System (CIMS) is a digital tool that allows law enforcement agencies to store, organize, and exchange information about criminal activity. [4] A CIMS network consists of multiple nodes, which are computers or other devices connected to the computer and running CIMS software. Each node in the CIMS network acts as a verifier of the information stored in the system. They are responsible for ensuring that any new data added to the system is valid and meets the standards of the CIMS network. Nodes can check the accuracy of existing data and share that information with other nodes. [2]

Minor nodes in the CIMS network play a unique role in the system. They add new data to

the system and create new blocks on the CIMS blockchain. This includes details of new crimes, suspects, or evidence. Miner nodes use computational power to solve complex problems that ensure the validity of information entered the system. Once a minor node successfully adds new data, it is permanently recorded and stored by every node in the network. In short, nodes in the CIMS network verify and transmit information, while minor nodes are responsible for adding new information and protecting the network from fraudulent activity.

Criminal Records deploys with blockchain based smart contract.

To deploy a criminal information management system (CIMS) using a blockchain-based smart contract, the first step is to determine the specific requirements and use case of the system. Once these are identified, a smart contract can be created to define the rules and logic of the CIMS network. The smart contract is stored on the blockchain and automatically executed under certain conditions. Whenever new data is added to the CIMS, the smart contract automatically checks the information and compares it to the rules of the network. This ensures that the data added to the system is valid and conforms to the network's standards. In addition, the smart contract can be used by different user types, such as B. Assign different roles and permissions to law enforcement officers, investigators, and administrators. [5] The use of blockchain technology and smart contracts gives the CIMS network a high level of transparency and immutability. Every change and transaction that takes place in the CIMS is recorded on the blockchain, making it easy to track the history of the data and prevent unauthorized changes or tampering.

3.4. Technologies used in the project.

- Node.js
- Ganache Personal blockchain
- Truffle Suite
- MetaMask Ethereum Wallet
- Solidity

9. Ethereum Virtual Machine for implement Smart contract.

The Ethereum virtual machine (EVM) is the execution environment for smart contract bytecode on the Ethereum blockchain network. EVM is run on every node in the network, enabling all nodes to perform the same computations and store the same values when executing transactions that point to smart contracts. Even transactions that only transfer balances require calculation to determine the balance of the address and deduct it accordingly. Each node performs transaction execution and stores the final state for various reasons.[3] For example, in a smart contract that records the names and details of party attendees, when a new person is added, a new transaction is sent across the network. Any node in the network can display details of all attendees simply by reading the final state of the contract. Every transaction requires computation and storage within the network.

10. Implement Smart contract with Encryption.

Several steps are required to implement smart contracts with encryption for a blockchain-based crime information management system. First, the encryption requirements must be defined, which includes identifying the specific data fields that require encryption and determining the encryption algorithms and key management protocols to be used. Once these requirements are established, an encryption engine must be developed in collaboration with a development team. This module should contain the encryption algorithms and key management protocols identified in the previous step. The next step is to integrate the encryption engine into the smart contracts, which involves writing code to invoke the encryption engine and thoroughly testing and debugging the code to ensure it is working properly. Once the smart contracts are developed and evaluated, they can be deployed on the blockchain, which requires coordination between technical teams and actors involved in the criminal justice system. Finally, it is important to monitor and evaluate the encrypted smart contracts to assess their impact on the criminal information management system. This could include analyzing data on record accuracy, turnaround times, and user satisfaction, and identifying issues that need to be addressed. [2]

Tools We Need: Ganache, Truffle, MetaMask, Solidity js, Knowledge of basic JavaScript etc.

11. Encrypted Chain of Block Architecture

The first block of a blockchain is known as the Genesis Block, which serves as the starting point for the subsequent blocks. Each block stores a reference to the previous block in the chain. However, as the Genesis Block is the first block, there is no previous block to reference. [1] Therefore, its hash value is set to 0, indicating that no data was processed before it. The following blocks are numbered sequentially, starting with one, and each block's previous hash value is set to the hash of the previous block, resulting in a unique hash for each block. This process continues until all blocks have been added to the blockchain. [1]

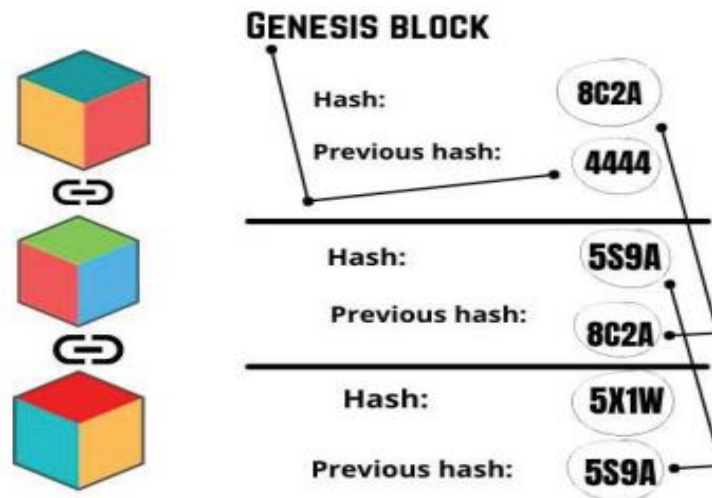


Figure 5: Structure of a blockchain [2]

3.5. Gantt Chart

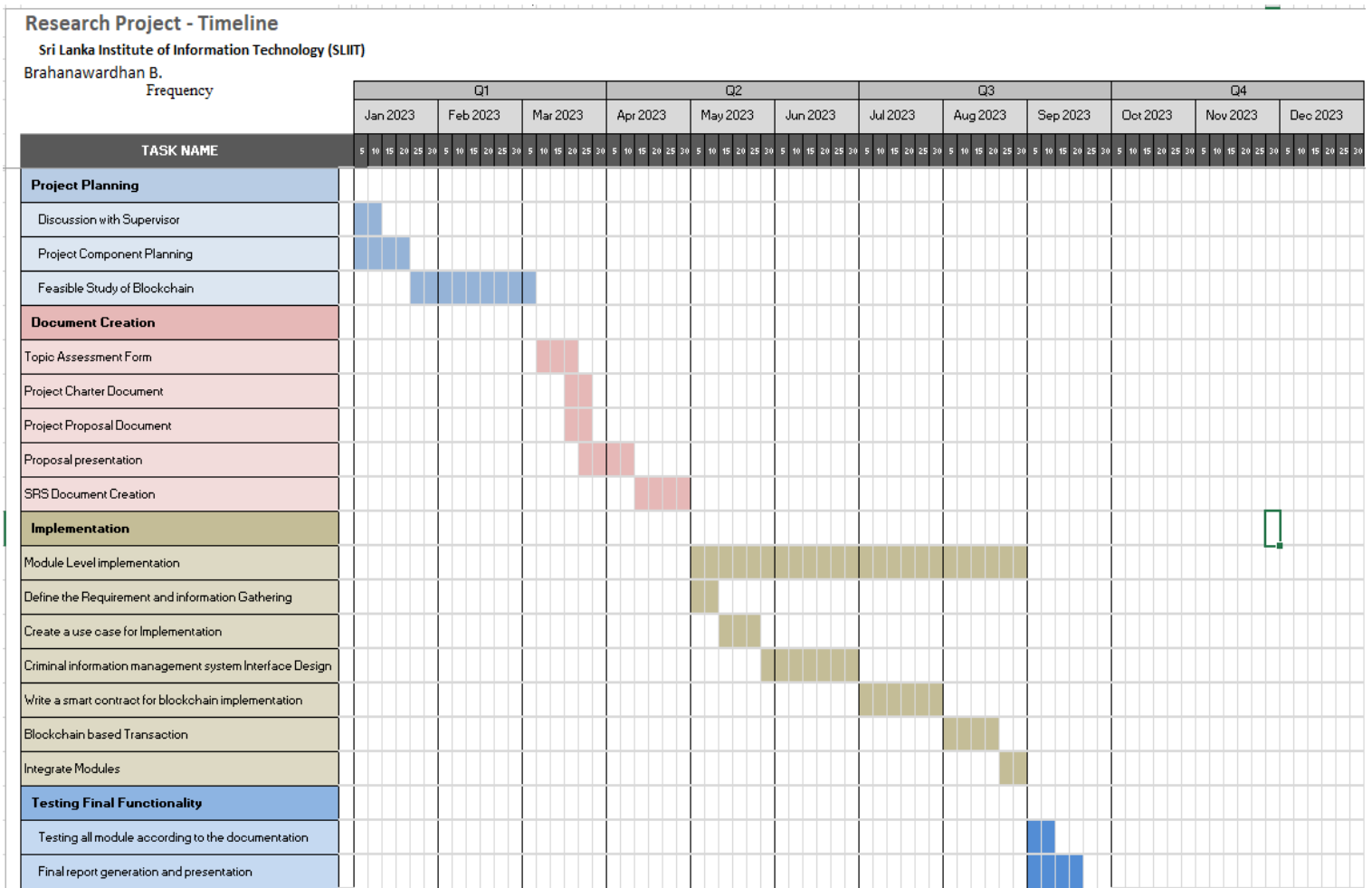


Table 1.2 Research Project Timeline

4. BUDGET

Table 1.3 – Research budget

| Expenses | Price (Rs.) | Price (\$) |
|--------------------|--------------------|-------------------|
| Server Hosting | 1700.00 | \$ 5.25 / Month |
| Research publishes | 10,000.00 | \$ 30 |
| Total | 11700.00 | |

5. Commercialization

Target Audience

- Throughout this product the primary target for our research product is we plan to market this product for only suitable industries only such as Law enforcement agencies, Private investigation, Police departments.
- The criminal information management system based on blockchain offers a secure, transparent, and efficient way to manage and share criminal information, while reducing the risk of data tampering.
- The pricing model is based on subscription tiers that vary based on the size of the organization, number of users, and level of customization. The branding and positioning of the system will highlight its reliability, security, and efficiency, and emphasize its ability to streamline criminal information management, enhance collaboration, and increase trust among agencies and parties.

Method of Gain Profit

- The blockchain based criminal information management system will under our maintenance service. We will provide customer support service and it will cost monthly charges for maintain the system and protect the confidential records from unauthorized parties.

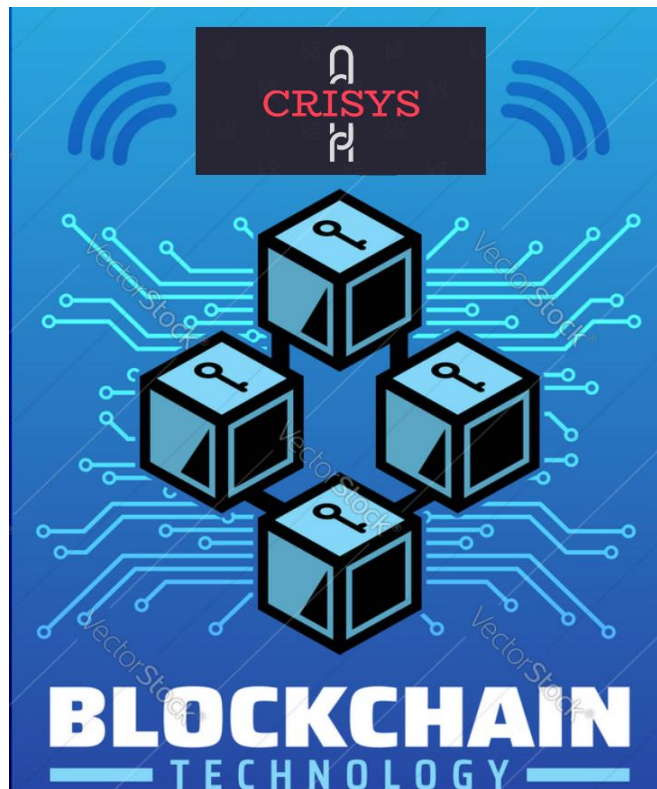


Figure 5: Commercialization Poster

6. Reference List

- [1] “Blockchain-based Criminal Record Database Management.” [Online]. Available: <https://ieeexplore.ieee.org/document/9544655>. [Accessed: 19-Mar-2023].
- [2] “Crab: Blockchain based Criminal Record Management System.” [Online]. Available: https://www.researchgate.net/publication/329489346_CRAB_Blockchain_Based_Criminal_Record_Management_System. [Accessed: 19-Mar-2023].
- [3] “Can blockchain strengthen the internet of things? - IEEE xplore.” [Online]. Available: <https://ieeexplore.ieee.org/document/8012302/>. [Accessed: 19-Mar-2023].
- [4] “Blockchain-based Criminal Record Database Management.” [Online]. Available: <https://ieeexplore.ieee.org/document/9544655>. [Accessed: 19-Mar-2023].
- [5] “Do you need a blockchain? | IEEE conference publication - IEEE xplore.” [Online]. Available: <https://ieeexplore.ieee.org/document/8525392>. [Accessed: 19-Mar-2023].
- [6] Wust, K., Gipp, B., & Breitenbücher, U. (2018). “Blockchain in forensic science: Securing digital evidence”. In 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) (pp. 1350-1355). IEEE.
- [7] Wang, L., Ma, X., Li, M., Li, J., & Wang, Y. (2020). “Design and implementation of a blockchain-based criminal case management system”. *Journal of Ambient Intelligence and Humanized Computing*, 11(1), 341-350

[8] Jain, A., Das, S., Kushwah, A. S., Rajora, T., & Saboo, S. (2021). Blockchain-Based Criminal Record Database Management. In 2021 Asian Conference on Innovation in Technology (ASIANCON) (pp. 1-5). IEEE.

[9] Badruddoja, S., Dantu, R., He, Y., Upadhayay, K., & Thompson, M. (2018). Making Smart Contracts Smarter. IEEE Computer, 51(9), 98-102. doi: 10.1109/MC.2018.3641025

[10] Abuhashim, A., & Tan, C. C. (2018). Smart Contract Designs on Blockchain Applications. In 2018 IEEE International Conference on Smart Computing (SMARTCOMP) (pp. 261-266). IEEE. doi: 10.1109/SMARTCOMP.2018.00047.

*******The End*******