BLOCKCHAIN BASED CRIMINAL INFORMATION MANAGEMENT SYSTEM IN SRILANKA

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

September 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	

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

…… ……...

Signature of the supervisor Date

(Mr. Kanishka Yapa)

…… ……..

Signature of the co-supervisor Date

(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

Table of Figures

List of Tables

List of Abbreviations

Abbreviation	Description
BCIMS	Blockchain based criminal information management system
USA	United States of America
AI	Artificial Intelligence
GDPR	General data protection act.
SIM	Subscriber Identity Module
NIST	National Institute of Standards and Technology
HTML	Hypertext Markup Language
JS	JavaScript
CSS	Cascading Style Sheets
HMAC	Hash-based Message Authentication Code
P2P	Peer to peer network
POW	Proof-of-work
SHA-256	Secure Hash Algorithm 256-bit
DApp	Decentralized Application
BaaU	Blockchain-as-a-utility
POS	Proof of Service
SC	Smart Contracts
TX	Transaction

List of Tables

1. INTRODUCTION

Criminal Information Management System is a vital component of any effective justice system. Crimes in our daily life are increasing to an uncountable level due to the current economic crisis that Sri Lanka is facing [1]. The daily life of the people in Sri Lanka is in a difficult situation due to allegations of activities like theft, money laundering, bribery, and extortion that are occurring daily due to people becoming criminals and dishonestly within police stations. Accusations are being covered up as they come due to politics and bribery. One of the main bottlenecks that police stations and departments are facing is the increased number of criminal records and how they can handle them efficiently. As far as Sri Lanka is concerned, the complaint handling and recording of criminal activities are mainly maintained manually and on a centralized system that covers technologically advanced areas.

Due to these limitations and the paper-based method, there are a considerable number of drawbacks and defects that police stations and departments are facing, and some of them are a limited amount of accessibility, lack of transparency, criminal records tampering, records misplacing, and many more. This has made it challenging for law enforcement organizations within Sri Lanka to effectively conduct and proceed with justice for criminals.

A potential remedy for these drawbacks is a method based on blockchain technology. Blockchains are distributed, tamper-resistant digital ledgers implemented without a central authority and are tamper-evident. In their most fundamental form, they enable a community of users to record transactions in a shared ledger within that community. As a result, no transaction can be altered after it has been published in the normal operation of the blockchain network.

Therefore, our team has proposed a “Blockchain-Based Criminal Information Management System” (CRISYS) to address the problem and challenges law enforcement organizations face in Sri Lanka. 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.

One of the primary discussions in the field of blockchain-based criminal information management systems concerns whether to use blockchain technology or regional centralized systems for the storing and interchange of criminal data. Local data repositories in the criminal justice field would necessitate that various law enforcement agencies and institutions retain data locally within their own controlled structures and databases, much like centralized systems in healthcare. However, implementing centralized criminal information management systems poses several serious problems that are similar to those in the healthcare industry.

Lack of Individual Control: In a centralized paradigm, the people whose criminal histories they relate to do not own or control those histories. In a perfect world, people would own and be in charge of their criminal histories.

Data fragmentation: As people engage with numerous law enforcement authorities, criminal records may become fragmented, much like medical information distributed among various medical facilities. Data fragmentation and a lack of a uniform, comprehensive system are caused by the replication of records across several entities.

Interoperability Challenges: Different law enforcement agencies frequently use dissimilar systems and databases for record-keeping, which creates compatibility and interoperability issues. The efficient exchange and use of criminal information is hampered by these systems' inability to fluidly communicate with one another.

Inefficient, Complex Data Sharing: Inefficient, Complex Data Sharing: Sharing criminal records among law enforcement agencies and relevant entities can be a convoluted and time-consuming process. This inefficiency not only delays critical investigations but also jeopardizes public safety.

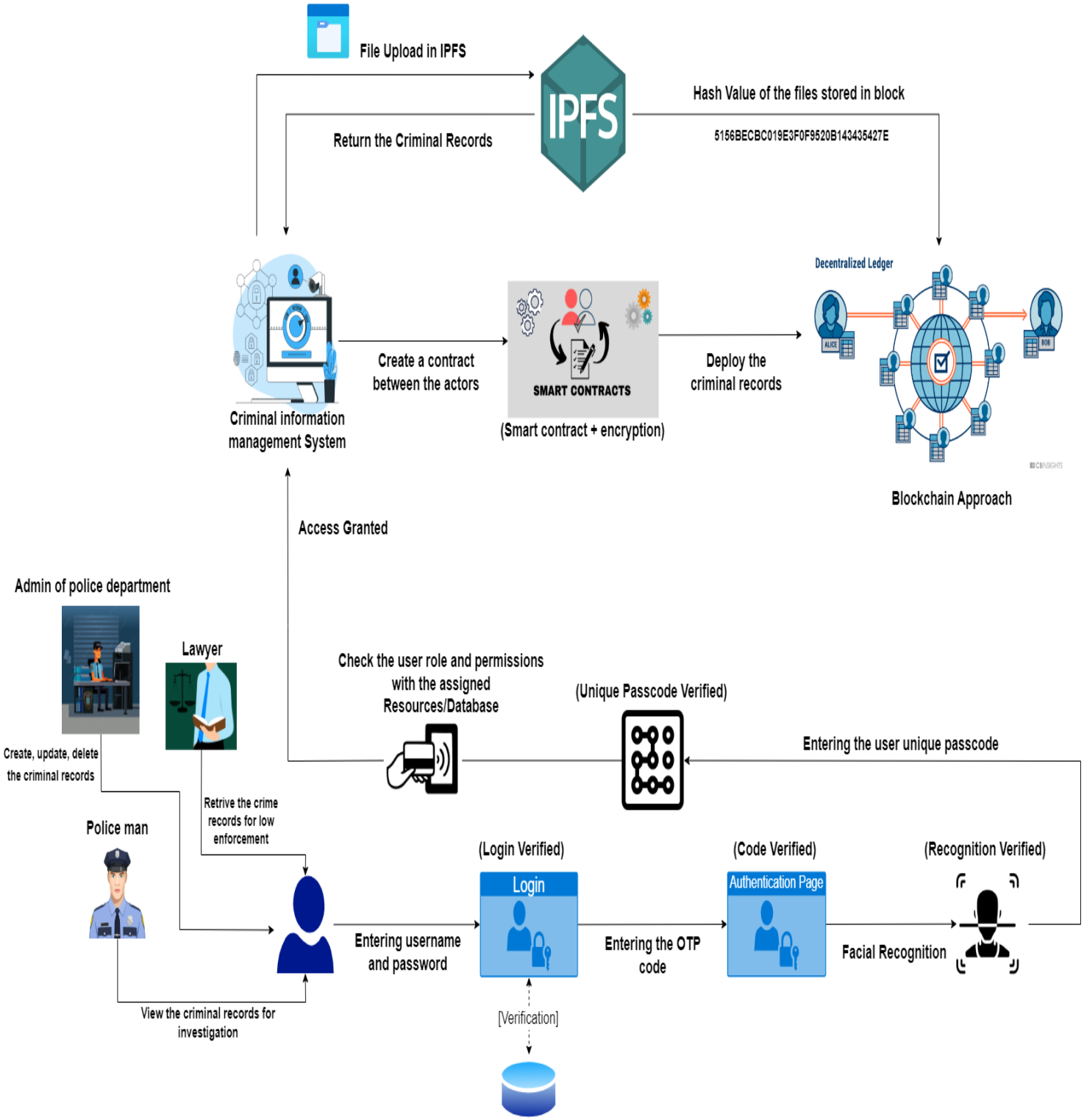


Figure 1: Complete System overview diagram

1.1.Background of study

Direct, a strong and secure email protocol, has been successfully used in the US to assure the encrypted delivery of data between numerous stakeholders, including law enforcement agencies and pertinent parties. The literature on Blockchain-based criminal records administration devotes a sizable portion of its pages to solving these problems. The creation of centralized frameworks and processes that enable the safe sharing of criminal histories across cloud-based infrastructures allows for this.

The blockchain was first made public as the underlying technology for Bitcoin, but it has now moved beyond its financial roots to become a focus of investigation for researchers and inventors. One such area where blockchain technology has enormous potential is the administration of criminal information. Its potential influence goes far beyond conventional financial applications, and its adoption is anticipated to have a large positive impact on the criminal justice system.

The application of blockchain technology to criminal information systems is a topic of growing interest and research in various countries, including Sri Lanka. While the concept of blockchain for managing criminal records has gained attention primarily for its security and transparency features, its implementation in Sri Lanka presents a unique set of challenges and opportunities. Sri Lanka, like many other nations, faces challenges related to centralized and outdated systems for managing criminal records. The need for a more efficient, secure, and transparent system is essential for maintaining law and order. Blockchain technology has the potential to address these challenges effectively.

In Sri Lanka, the adoption of a blockchain-based criminal information management system could significantly improve data accuracy and accessibility. A decentralized ledger would ensure that records are tamper-proof, reducing the risk of corruption or unauthorized alterations. Additionally, the transparent nature of blockchain would promote trust among law enforcement agencies, legal authorities, and the general public. Furthermore, blockchain technology can facilitate seamless information sharing between various stakeholders involved in the criminal justice system, such as the police, courts, correctional facilities, and government agencies. This would streamline the process of criminal record verification, aiding in more efficient investigations and legal proceedings. However, it is important to acknowledge that implementing a blockchain-based system for criminal information management in Sri Lanka

would require careful planning, investment in technology infrastructure, and regulatory frameworks. The legal and ethical aspects of data privacy and consent must also be thoroughly considered to protect the rights and privacy of individuals.

To gain deeper insights into the potential and challenges of implementing a blockchain-based criminal information management system in Sri Lanka, researchers and policymakers should explore the existing literature on blockchain applications in criminal justice and adapt these findings to the specific needs and circumstances of the country. Additionally, case studies and pilot projects can help assess the feasibility and practicality of such a system in the Sri Lankan context. In conclusion, the adoption of blockchain technology for managing criminal information in Sri Lanka has significant potential to improve the efficiency, security, and transparency of the criminal justice system. However, careful planning, investment, and consideration of legal and ethical implications are necessary to harness its full potential in the Sri Lankan context. Further research and collaboration with experts in the field will be essential to successfully implement and leverage this innovative technology.

1.2. Literature Review

1.2.1. Web3 Concept

At the start of internet, the Web 1.0, initial internet concept was based on open source and static content. Those who had content digitized them, organized, and sent out to published publicly. Web 1.0 had basic features of internet and restricted mainly due to slow and poor connectivity, the issues with infrastructure and technological limitations. Launching of graphical user interface along with Mozilla (Netscape) web browser was the initiation for Web 1.0 [7].

Figure 2: Web 1.0 (1990-2004) Read Only

Evolution in to Web2.0 was more promising with user generated content and centralized applications. It is more dynamic and interactive. Connectivity improved, and the people start living in the era of internet dominated by social media. The concern arose when the data ownership was not on the user side, but with the involvement of 3rd parties and their contracts. Web 2.0 permitted free flow of information specially with the improvement of messaging services and freely available secure applications. Hence Web 2.0 allows people to have easy access to internet and to be interactive and learn almost anything on it.

Figure 3:Web 2.0 (2004 – present) – Read/Write

Significance of web 3.0

1. Edge computing – a distributed IT architecture that enables some resources and processes from cloud and data centers closer towards the source. This helps in reducing latency and the use of bandwidth. Users producing more data as they own laptops, phones, appliances, sensors, and many other units of data creation, an optimization over the bandwidth usage and latency is required.
2. Decentralization – instead of large, centralized data locations, Web 3.0 allows a distribution among builders and users. Refers to more control for data owners and protect data privacy and ownership.
3. Permissionless – Anyone on internet can join a blockchain anonymously, make transactions and store data on it when other participants validate it. In essence, everyone gets equal opportunity to participate in activities.
4. Native payment currency – spending and receiving on online transactions are based on crypto currencies which has eliminated the involvement of third parties such as banks and their outdated infrastructure [8].

5. Trustless but verified – no reliance on third parties, therefore validations and verification done by consensus mechanisms and extensive security features which eliminate the need for trust

Main limitation of web3.0 concept as at today can be identified as the pacing development of the concept. The dependency on current centralized infrastructure and the web3 organizations urging to fill the gaps does not result in stable and reliable infrastructure solutions. Secondly, the accessibility of web 3.0 over the low-income countries due to relatively high transaction costs. Currently Ethereum is working on reducing the transaction costs via scaling and upgrading solutions. Currently high technicality on documentation and the use and operation of wallet concepts are also limitations of useability of web3.0 concepts, those which are improving with the new developments and concepts.

1.2.2. Overview of blockchain

The concept of blockchain technology originated with the introduction of the digital payment system that underpins Bitcoin cryptocurrency. Essentially, blockchain is a sophisticated technology designed to oversee and manage transactions by storing, verifying, and validating them within a decentralized database system.

Bitcoin is a form of digital currency that mirrors physical money but exists solely in a digital format. It serves as a medium for direct buying, selling, and exchanging of value, all within a decentralized framework. The fundamental aim of digital currencies like Bitcoin is to ensure transparency in financial transactions. Within the realm of digital currency payments, each transaction undergoes a meticulous process of verification, storage, and secure locking within digitally distributed ledgers, accessible to anyone interested.

This secure and unalterable recording of transactions is what fosters the transparency Bitcoin advocates for. Furthermore, the management of transactions by network nodes effectively eliminates the necessity for trusted intermediaries such as banks. At its core, Bitcoin relies on a distributed digital record known as the blockchain. This blockchain consists of a chain of connected records, or "blocks," each of which is open for public viewing. These blocks contain comprehensive information about the transactions that have taken place, and they are linked together in chronological order, forming a digital chain of blocks. The incorporation of

cryptographic security techniques into the digital currency and blockchain concept significantly reduces the risk of false or unauthorized payments [9].

In essence, blockchain technology, initially conceived for Bitcoin, has evolved into a transformative innovation with far-reaching implications for various industries beyond cryptocurrencies, offering enhanced security and transparency in transaction management.

Blockchain technology offers several significant benefits to its network users:

1. Transparency and Decentralization: Transactions conducted on a blockchain operate transparently and are publicly accessible for anyone to read and validate. This eliminates the need for a central authority or intermediary to oversee and validate transactions, thereby promoting a decentralized ecosystem.
2. Efficiency and Speed: The transparency of transactions and the absence of a third-party intermediary enable faster processing and exchange of information. This efficiency can lead to quicker transaction settlements and enhanced information sharing.
3. Data Privacy and Public Availability: Blockchain technology strikes a unique balance by allowing information to be owned anonymously while remaining publicly available. This ensures data privacy for individuals or entities while still enabling transparency and verification by the wider community [10].

The core strength of the blockchain concept lies in its ability to maintain records in a distributed and immutable manner. This immutability forms the foundation for implementing secure and unchangeable ledger systems. Consequently, blockchain technology is finding applications beyond the realm of financial processes.

Platforms like Ethereum and Hyperledger exemplify decentralized applications tailored for business purposes [11]. Industries such as e-health records, validation processes (such as degree certificates and music royalties), voting systems, and numerous other domains are increasingly considering blockchain technology to enhance their processes and ensure data integrity and transparency. This expansion of blockchain's utility reflects its versatility and potential to bring about transformative improvements in various sectors.

1.2.3. Types of Blockchain

Blockchain networks can be categorized into four primary types based on their structure: Public, Private, Permissioned, and Consortium Blockchains.

Public Blockchain: In a public blockchain, the network is open to anyone who wishes to join and participate in transactions. While it offers inclusivity, it presents challenges such as high computational power requirements and reduced transaction privacy due to the visibility of transactions to a broad audience. Despite these issues, public blockchains employ cryptographic functions and consensus algorithms to ensure security. Notable examples of public blockchains include Ethereum and Bitcoin.

Private Blockchain: A private blockchain combines the features of a decentralized peer-to-peer network with those of a public network. However, it differs in that it has central management overseeing the network, controlling participation, and maintaining the ledger. This central authority element can enhance trust among participants. Importantly, a private blockchain can be hosted on-premises behind a firewall, providing organizations with a higher level of data security. Essentially, it functions as a distributed system with robust security measures and embraces the fundamental principles of blockchain data storage.

Permissioned Blockchain: Every private blockchain is inherently a permissioned blockchain. In a permissioned blockchain, participation is restricted, typically through invitations or permissions granted to individuals or organizations. Even within a public blockchain network, organizations can opt to set up a permissioned blockchain to bolster security and privacy further. This approach allows for a more controlled and secure environment.

Consortium Blockchain: A consortium blockchain enables multiple organizations to collaborate on a single blockchain network. Participants in this type of network are granted permissions to participate, and the responsibility for managing the blockchain is shared among the consortium members. This model is particularly useful when multiple entities need to collaborate, and decisions about who can transact and view the blockchain are made collectively by the consortium [12].

Choosing the appropriate blockchain type is a critical consideration for enterprise-level blockchain implementations. Factors such as security, openness, and the specific requirements of the organization must be carefully evaluated to determine which blockchain structure aligns best with the desired outcomes. Each type of blockchain offers its unique advantages and trade-

offs, making it essential to make an informed decision when selecting the most suitable blockchain for a given application or use case.

1.2.4. Blockchain Concept

In simple terms, blockchain serves as a digital ledger designed to record and validate information through the consensus of its participants, ensuring data integrity and making it extremely resistant to tampering or deceit. Put differently, blockchain can be likened to a "tamper-evident" and "tamper-resistant" digital ledger system, typically implemented in a decentralized manner and devoid of central control [13].

The genesis of this concept can be traced back to the inception of Bitcoin cryptocurrency, which was conceived as a payment scheme aimed at eliminating the need for third-party intermediaries. Traditional payment models relied on trust but incurred higher transaction costs due to the involvement of financial institutions and the collection of excessive personal and confidential information [14]. Blockchain-based cryptocurrency systems successfully address these weaknesses.

Within a peer-to-peer (P2P) distributed blockchain network, a "node" plays a crucial role. These nodes are open-source, cross-platform runtimes [15] that actively participate in the blockchain ecosystem. Broadly, there are three types of nodes:

Full Nodes: These nodes maintain a complete and unaltered copy of the entire blockchain. They do so to ensure the security, integrity, and accuracy of the blockchain. Full nodes also have the capability to publish new blocks.

Publishing Nodes: A subset of full nodes, publishing nodes possess the ability to create and publish new blocks in the blockchain. Their role is vital in the ongoing operation of the blockchain network.

Lightweight Nodes: Unlike full nodes, lightweight nodes do not maintain a complete copy of the blockchain. Instead, they connect to a full node and synchronize themselves with the current state of the blockchain. Lightweight nodes then relay their transactions to the full node [13].

As blockchain technology continues to advance rapidly, the requirements for deploying nodes have evolved. Unlike the early days when running a node could be achieved with low-performance equipment, today's demands emphasize memory and processing power as crucial

factors [15]. Different blockchain networks may impose their own specific requirements for node deployment, which can vary based on the network's operations and needs.

In essence, publishing nodes play a pivotal role in the creation and attachment of blocks to the blockchain, contributing to the network's ongoing functionality and integrity. The evolution of node deployment requirements underscores the growing importance of robust hardware specifications in the contemporary blockchain landscape.

Figure 4 shows the structure of a block and Figure 2.5 shows how the blocks are connected in the blockchain. The initial block – genesis block has no parents and other blocks are chained to their parents via the parent block hash.

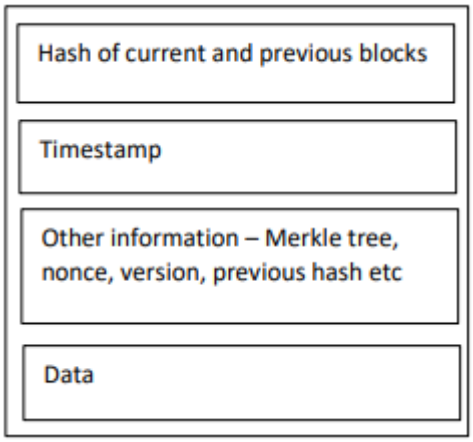


Figure 4:Sample Structure of a block

Figure 5 depicts how blocks are chained to make a blockchain. The hash digest of the previous block header is included in the new block, thus chaining it to the previous block. Hence an altered block can easily be detected and rejected from the chain effectively. The body of a block contains the transaction counter and transactions.

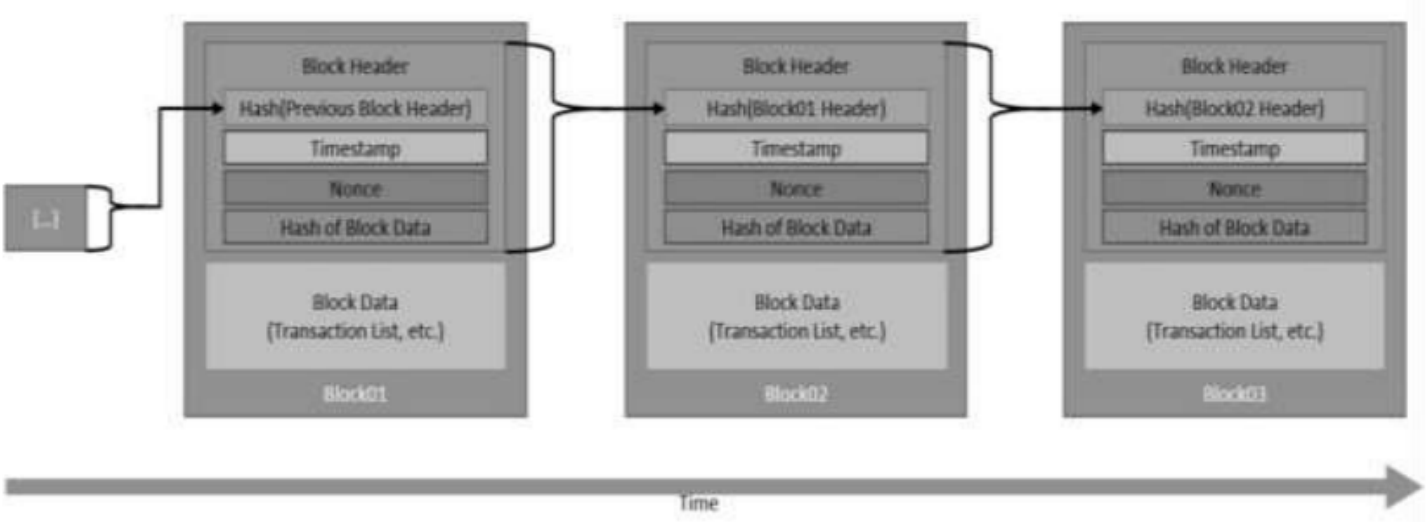


Figure 5:Generic Blockchain [13]

Table 1:Blockchain Components Details

Block header components	Description
Block Version	Indicate what version of blockchain is being used in the network. Version 1.0 – Cryptocurrency. Use a public ledger to store data (Ex. Bitcoin) Version 2.0 – Smart contracts. Self-executing programs (Ex. Ethereum) Version 3.0 – Decentralized Applications Version 4.0 – Blockchain for industry. To develop scalable and affordable networks to be used in the industry.
Merkle tree root Hash	Hash value of all the transactions in the block
Timestamp	Current time in seconds as from January 1,1970. Used as a serial number, gives out the time the block has been mined and validated. Can also use to verify the authenticity of the block.
nBits	Compressed representation of the threshold value of the block's hash.
Nonce	A 4-byte random number changed by mining and once confirmed, used in calculating the block hash

Parent Block	Hash value of the previous block

A distributed digital ledger is a chain of interconnected blocks that contains transaction information. It embodies the fundamental characteristics of traditional financial ledgers but offers several advantages over centrally based ledgers.

1. Redundancy and synchronization: Multiple copies of the ledger are maintained across various locations, all of which remain synchronized. This ensures that the ledger is always available and that no single point of failure exists.
2. Network heterogeneity: The diverse composition of the network provides protection against attacks on individual nodes, enhancing overall ledger security. This is because no single entity controls the network, making it difficult for attackers to target.
3. Geographical dispersion: The geographical distribution of nodes reduces the risk of data loss due to node failure or regional issues. This is because the ledger is not stored in a single location, so if one node fails, the others can still access the data.
4. Transaction validation: Each transaction undergoes validation by multiple nodes, allowing the network to reject malicious transactions or those from compromised nodes, thereby ensuring the accuracy of the ledger. This is done through a consensus mechanism, which is a process by which all nodes in the network agree on the validity of a transaction.
5. Tamper resistance: Blockchain employs cryptographic features to create a tamper-evident and tamper-resistant ledger. This means that it is very difficult to alter or delete data once it has been added to the ledger.
6. Immutable records: Users can only append blocks to the ledger, making it impossible to alter existing information. This ensures that the ledger is always accurate and reliable.

Every blockchain user possesses both a private key and a public key. The private key is used for digitally signing transactions, while the public key is used to verify signatures. These digitally signed transactions are distributed across the network. Blockchain relies on the Elliptic Curve Digital Signature Algorithm (ECDSA) for this purpose.

Transactions in the context of blockchain refer to interactions between various parties or participants within the blockchain. In the case of cryptocurrencies, a transaction involves the transfer of cryptocurrencies between two parties. In a business context, it may involve the recording of activities related to an asset. The specifics of a transaction's data can vary depending on the implementation and business logic, although the transaction process generally adheres to a standard format. Typically, a transaction includes sender identification, sender's public key, digital signature, transaction inputs, and outputs.

There are three primary categories of blockchains: public, private, and consortium.

Public blockchains: These are permissionless blockchains that allow anyone to participate in the consensus process, and the records are publicly visible. Public blockchains are open-source and freely accessible for download. However, their openness also makes them more susceptible to malicious attacks, necessitating the implementation of strict consensus rules.

Permissioned blockchains: Permissioned blockchains require authorization from a designated authority to publish a node. Private blockchains fall into this category, often resembling a centralized network within an organization.

Consortium blockchains: Consortium blockchains combine elements of both private and public blockchains. Some nodes are granted permission to publish, offering a balance between control and transparency in the blockchain network.

1.2.5. Consensus Algorithms

The main challenge in a blockchain is to reach consensus on which node will add the next block to the chain. This is especially difficult in permissionless blockchains, where nodes do not trust each other and are motivated by financial gain. As a result, conflicts can arise when multiple nodes try to add the same block to the chain at the same time. To resolve these conflicts, blockchains use consensus algorithms. Consensus algorithms are a set of rules that all nodes in the network agree to follow in order to determine which node will add the next block. There are many different consensus algorithms, each with its own advantages and disadvantages. In permissionless blockchains, consensus algorithms are typically resource intensive. This is because nodes need to invest significant resources in order to have a chance of being selected to add the next block. Resources can include computational power, time, and storage space. In contrast, permissioned blockchains typically use less resource-intensive consensus algorithms. This is because nodes in permissioned blockchains are typically known

to each other and trust each other to some degree. As a result, there is less need to invest significant resources in order to secure the network. The choice of consensus algorithm depends on the specific requirements of the blockchain. For example, permissionless blockchains that require high levels of security may use a more resource-intensive consensus algorithm, such as Proof of Work. Permissioned blockchains that are less concerned with security may use a less resource-intensive consensus algorithm, such as Proof of Stake.

Following is an evaluation of some of the consensus algorithms used

Proof of Work Consensus (PoW) model specifies, to publish a block, user need to solve a computationally difficult mathematical problem.

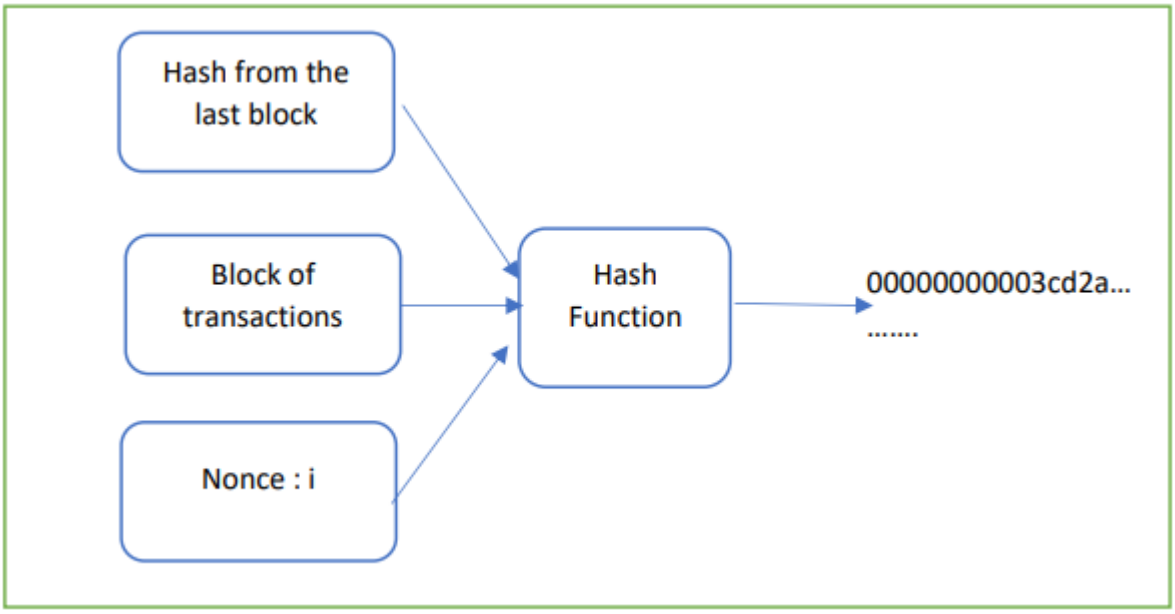


Figure 6:Proof of work Example

le

will add the next block to the chain. In PoW, nodes compete to solve a complex mathematical puzzle. The first node to solve the puzzle is rewarded with a cryptocurrency and is allowed to add the next block to the chain.

PoW is a resource-intensive consensus mechanism, requiring nodes to invest significant amounts of computational power and electricity. However, it is also a very secure consensus mechanism, making it difficult for attackers to manipulate the blockchain.

Proof of Stake (PoS) is a more energy-efficient consensus mechanism than PoW. In PoS, nodes are selected to add blocks to the chain based on the amount of cryptocurrency they hold. The more cryptocurrency a node holds, the more likely it is to be selected to add a block.

PoS is a less secure consensus mechanism than PoW, but it is also less resource intensive. This makes it a more attractive option for blockchains that are concerned about energy consumption.

Both PoW and PoS have their own advantages and disadvantages. The choice of which consensus mechanism to use depends on the specific requirements of the blockchain.

Table 2:Key differences between pow and pos

Consensus Mechanism	Pros	Cons
Proof of Work (PoW)	Secure, resistant to Sybil attacks	Resource-intensive, energy-intensive
Proof of Stake (PoS)	Less resource-intensive, energy-efficient	Less secure, susceptible to 51% attacks

In addition to PoW and PoS, there are a number of other consensus mechanisms that are being developed. These include Proof of Authority (PoA), Proof of Capacity (PoC), and Proof of Burn (PoB).

The choice of consensus mechanism is a complex decision that should be made on a case-by-case basis. The specific requirements of the blockchain, such as its security, scalability, and energy consumption, should be carefully considered when making this decision.

i. **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 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."

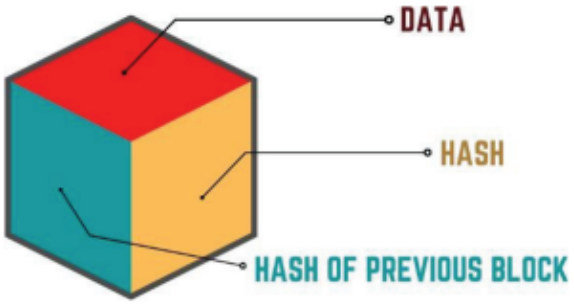


Figure 8:A Block [2]

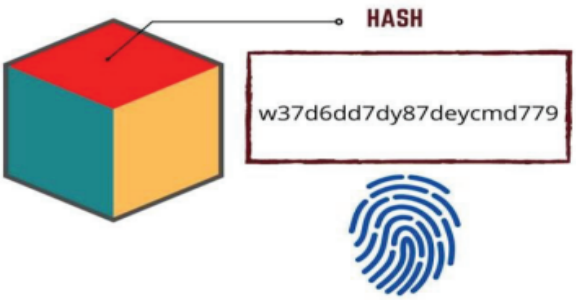


Figure 7: Hash in a Block [2]

1

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.

a. 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 Sri Lanka 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 number 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 evidence 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 12 blockchain in a 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 3: 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	MEDIUM	HIGH
Decentralization Of System	LOW	HIGH
Ensure data Integrity	MEDIUM	HIGH
Prevent loss of data	MEDIUM	HIGH
Availability	LOW	HIGH
Confidentiality	MEDIUM	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.

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.

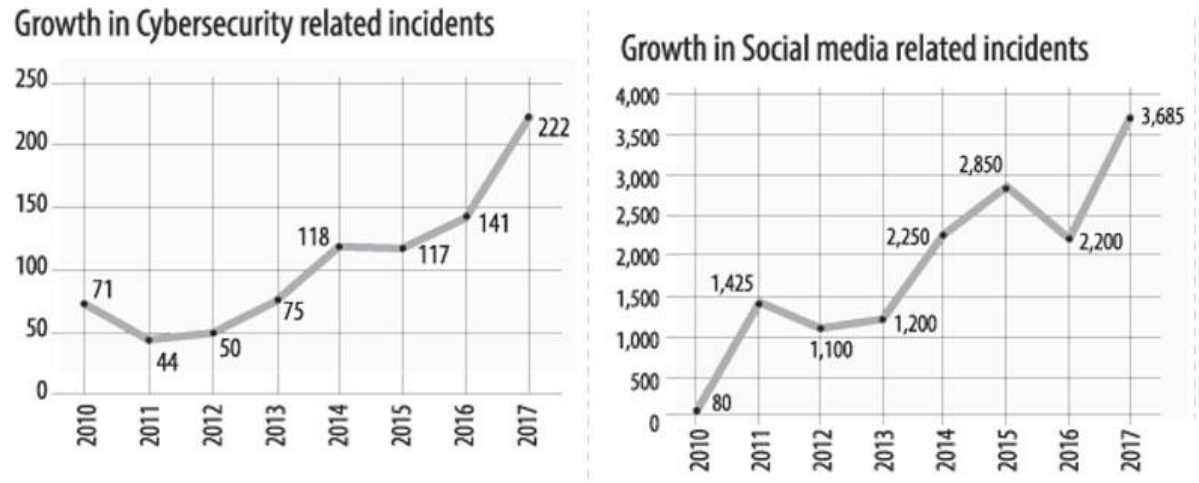


Figure 9:Increasing rates of criminal records in Sri Lanka

The growing global interest in blockchain technology for enhancing the management of criminal records has not yet been matched by research on its practical implementation and adaptation in Sri Lanka. While blockchain technology has the potential to improve data security, transparency, and information sharing in the criminal justice system, there is a lack of empirical studies, frameworks, and guidelines tailored to Sri Lanka's unique legal, cultural, and technological landscape.

This research gap necessitates a comprehensive investigation into the feasibility, challenges, and benefits of transitioning from conventional centralized criminal record management systems to blockchain-based solutions, taking into account the specific requirements and regulatory considerations of Sri Lanka. Addressing this research gap is essential to inform policymakers, law enforcement agencies, and stakeholders in Sri Lanka about the potential benefits and pitfalls of adopting blockchain technology in criminal information management and to develop a contextually appropriate framework for its successful integration.

The research gap on the practical implementation and adaptation of blockchain technology in Sri Lanka's criminal justice system can be attributed to the following factors:

- **Limited localized research:** There is a scarcity of studies that specifically address the Sri Lankan context, including its legal framework, cultural nuances, and technology infrastructure.
- **Adaptation challenges:** Sri Lanka's existing criminal records system may differ significantly from those in countries where blockchain implementations have been studied. There is a lack of guidance on how to adapt and integrate blockchain technology seamlessly into these distinct systems.
- **Regulatory and legal frameworks:** The legal and regulatory aspects of adopting blockchain for criminal record management in Sri Lanka remain largely unaddressed. There is a need to develop appropriate legal frameworks, compliance mechanisms, and data privacy regulations tailored to the country's needs.
- **Public perception and trust:** Public acceptance and trust in the blockchain-based criminal information management system are paramount. Research has shown that public perceptions of technology can significantly impact its success. There is a need to examine how Sri Lankan citizens and stakeholders perceive blockchain technology in the context of handling sensitive criminal information and how this perception can be positively influenced.

- **Cost-benefit analysis:** There is a need to conduct a comprehensive cost-benefit analysis to assess whether the financial investments required for the implementation of blockchain technology are justified within Sri Lanka's budgetary constraints.
- **Stakeholder collaboration:** Understanding the dynamics of stakeholder collaboration is essential for the successful adoption of blockchain-based systems. There is a need to investigate how various agencies, including law enforcement, judiciary, and government bodies, can work together effectively in the context of blockchain.
- **Scalability and long-term viability:** It is crucial to ensure the scalability and long-term viability of a blockchain-based criminal information management system. Researchers need to investigate whether the technology can accommodate the increasing volume of data over time and whether it can remain relevant in the face of evolving criminal justice needs and technological advancements.

b. 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.

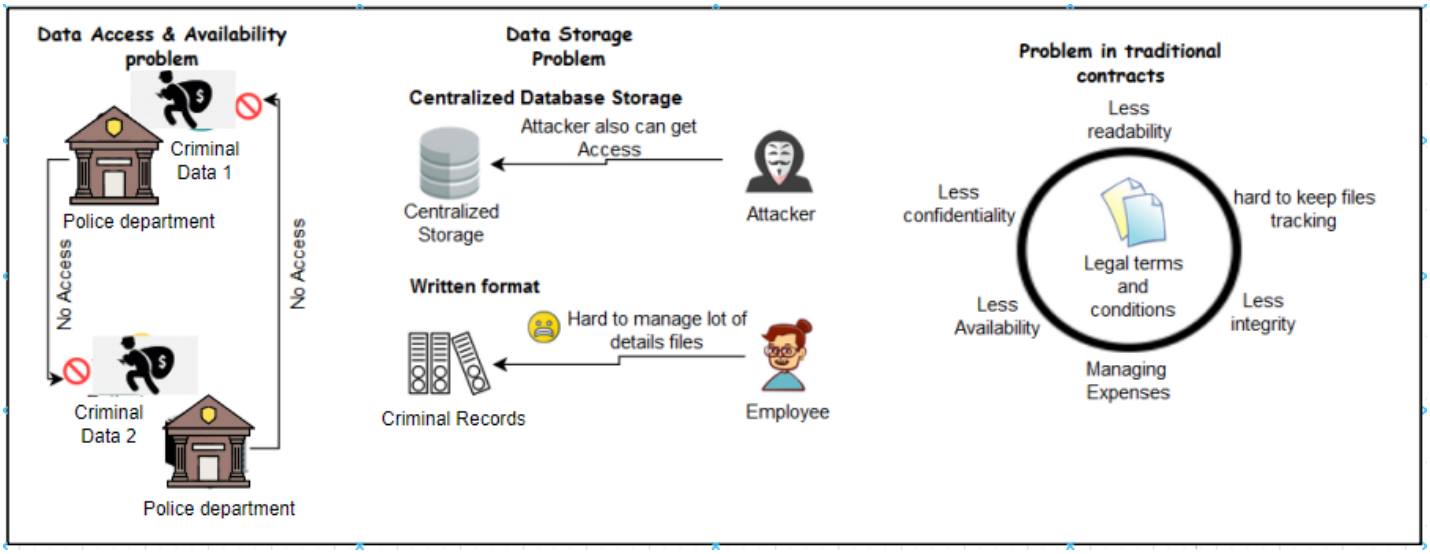


Figure 10:Common Problem that faced in Current Criminal System

In addition to addressing the pressing issues of data security and transparency, a blockchain-based criminal information management system offers several other significant advantages.

- **Enhanced accessibility and efficiency:** Blockchain technology can streamline the process of retrieving and sharing criminal records, making it more efficient and accessible for law enforcement agencies and relevant stakeholders.

- **Trust and reliability:** Blockchain's immutability ensures that once data is recorded, it cannot be altered or deleted without proper authorization. This safeguards the integrity of criminal records and reduces the risk of unauthorized data changes.

- **Automation and efficiency:** Smart contracts can be programmed to automate routine tasks, such as record updates, notifications, and data verification. This can save time and resources and contribute to the overall reliability of the system.

- **Citizen engagement and empowerment:** Individuals can have greater control and transparency over their own records, allowing them to verify and dispute information when necessary.

These advantages make blockchain a promising technology for improving the management of criminal information. However, it is important to note that blockchain is not a silver bullet and there are still some challenges that need to be addressed, such as the need for legal and regulatory frameworks, and the need to ensure data privacy and security.

The adoption of blockchain technology for criminal information management is a promising development with the potential to improve data security, transparency, and efficiency. However, there are still a number of research problems that need to be addressed before blockchain can be widely adopted in this context. One of the key challenges is the need to develop appropriate legal and regulatory frameworks. Blockchain is a relatively new technology, and its legal implications are still being debated. It is important to ensure that blockchain-based criminal information management systems are compliant with relevant laws and regulations, to protect the rights of individuals and to prevent the misuse of data.

Another challenge is the need to ensure data privacy and security. Blockchain is a distributed ledger, which means that data is shared across multiple nodes. This makes it more difficult to tamper with data, but it also raises concerns about data privacy. It is important to develop mechanisms to protect the confidentiality and integrity of data stored on blockchain, to safeguard the rights of individuals.

Finally, there is the challenge of scalability. Blockchain is a computationally intensive technology, and it can be difficult to scale to meet the needs of large-scale criminal information management systems. It is important to develop efficient and scalable blockchain solutions that can be used to store and manage large amounts of data.

The adoption of blockchain technology for criminal information management is a promising development with the potential to improve data security, transparency, and efficiency. However, there are a number of research problems that need to be addressed before blockchain can be widely adopted in this context.

- How can blockchain technology handle the increasing volume of criminal information records over time? This is a challenging problem, as blockchain is a distributed ledger technology that requires all nodes in the network to store the entire ledger. As the volume of data increases, this can put a strain on the network and make it more difficult to maintain data security and integrity.

- How can blockchain-based criminal information management systems be integrated with legacy systems used by law enforcement agencies? This is another challenging problem, as legacy systems are often not designed to be compatible with blockchain technology. There is a need to develop methods for integrating these systems in a way that ensures a smooth transition and minimizes data loss or disruption.

- What are the legal and ethical implications of storing sensitive criminal information on a blockchain? This is a complex issue that needs to be carefully considered. On the one hand, blockchain can offer significant benefits in terms of data security and transparency. On the other hand, there are concerns about the privacy of individuals and the potential for misuse of data.
- What are the trade-offs between decentralization (blockchain) and centralization (traditional systems) in terms of cost-effectiveness, efficiency, and security when managing criminal records? This is an important question that needs to be answered to determine the best approach for storing and managing criminal information.
- What are the methods for secure authentication and identity verification within a blockchain-based system to prevent unauthorized access while maintaining user privacy? This is a critical issue, as it is essential to ensure that only authorized users have access to criminal information.
- How do different blockchain governance models and consensus algorithms impact the trust, transparency, and overall performance of criminal information management systems? This is an important question, as the choice of governance model and consensus algorithm can have a significant impact on the security and performance of a blockchain-based system.
- **How can the usability of blockchain-based systems for law enforcement personnel be improved?** This is an important issue, as the usability of these systems will have a significant impact on their adoption and success.
- **What are the challenges and opportunities of using blockchain technology to facilitate secure cross-border sharing of criminal information, especially in cases involving international criminal investigations?** This is a promising area of research, as blockchain could offer a secure and efficient way to share criminal information across borders.

- **What are the potential cybersecurity threats and vulnerabilities specific to blockchain-based systems for criminal records?** This is an important issue, as it is essential to understand the risks associated with blockchain technology in order to mitigate them effectively.

- **What is the cost-benefit analysis of implementing blockchain technology for criminal information management?** This is an important question, as it is necessary to weigh the costs and benefits of this technology before it can be widely adopted.
- **How does public perception of blockchain technology impact its adoption in the criminal justice system?** This is an important question, as public trust is essential for the successful adoption of this technology.
- **What are the regulatory requirements and legal framework necessary for the adoption of blockchain-based criminal information management systems?** This is an important question, as the adoption of this technology will need to comply with relevant laws and regulations.
- **What are the specific challenges faced by developing nations, like Sri Lanka, in implementing blockchain solutions for criminal records?** This is an important question, as developing nations may face unique challenges in adopting this technology.

c. Research Objectives

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.

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 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.

2. Methodology

The purpose of the research is to clearly identify a verifiable solution to the problem of improving and security of the confidential criminal records stored by the police department in Sri Lanka. Existing manual methods has posed issues with regards to time waste, fraud, and miss use of the criminal records in the police departments. So we developed the solution using blockchain technology for addressed the problems currently facing (Interoperability, Handfill documents, Scattered Data, transparency of the records) in the existing Criminal records system in Sri Lanka.

A multifaceted strategy is used in the research plan and architecture to investigate developing a blockchain-based criminal information management system. To get 2 perspectives on current developments, systems, and optimal procedures connected to criminal information management and blockchain technology, an in-depth body of research will be undertaken first. This will provide a starting point for determining the gaps and difficulties that the suggested solution seeks to address. To fully comprehend the needs, demands, and concerns of important stakeholders, including law enforcement organizations, legal professionals, and technological specialists, interviews will also be performed with them. To learn about their opinions about the present criminal information management system and what they anticipate from a blockchain-based solution, a survey questionnaire will also be given out to prospective users [9].

To provide insightful conclusions, the data gathered through interviews and surveys will be examined using both qualitative and quantitative techniques. Based on the results, a blockchain-based criminal information management system prototype will be created and put through rigorous testing in a monitored environment. Through exercises and input from users, the system's functionality and usability will be assessed. The findings will be examined, and suggestions for enhancement, scalability, and potential difficulties will be made. A thorough examination of the viability, efficacy, and possible advantages of a blockchain-based criminal information management system in expanding the effectiveness and security of criminal data management operations will be ensured by the approach used.

The use of several innovative methods and technologies was required for the creation of a blockchain-based criminal information management system. Ganache, a private blockchain platform that is used in this system to manage criminal records, offers a secure and scalable

infrastructure. An agile paradigm was used for the process of developing software, enabling iterative development, constant feedback, and quick adaptability to changing needs.

Therefore, the methodology of solution should consider,

- Ensure the data Confidentiality, Integrity, and availability of managing criminal records.
- Smart contracts are self-executing contracts that are stored on the blockchain. They can be used to automate a variety of tasks, including data updates and revisions.
- Data immutability is the property of data that cannot be changed or deleted once it has been added to the blockchain. This is one of the key features of blockchain technology that makes it a secure and tamper-proof ledger.
- Controlled data changes: Smart contracts can be used to define the rules that govern how data can be changed. This ensures that data changes are made in a controlled and auditable manner.
- Smart contracts can be used to track all changes that have been made to data. This allows for data changes to be audited and verified.
- Enable a faster, secure, and reliable management for Criminal Records.

A smart contract based blockchain solutions was proposed to,

To ensure the anonymity of personal information, such as beneficiary and request information, which is sensitive and crucial, end-to-end encryption should be used.

The distributed ledger concept ensures that an exact copy of the information is distributed to all parties, making it difficult for adversaries to alter a single copy and reflect the fraud in all copies. This allows all participants to have full transparency and access to the entire transaction history.

The latency associated with manual methods, the possibility of human errors, and the involvement of third parties can be eliminated, resulting in improved efficiency and response time.

Once pre-specified conditions are met, transactions can be automatically approved and added to the storage without human intervention, which maintains immutability and reduces human involvement in sensitive or secure data transfers.

Finally, the solution should be future-proof and scalable to meet future needs. Blockchain and smart contracts are well-suited for this purpose, as they are the future of web3.0 and can easily support the solution's requirements.

2.1.Functionality

The system as for demonstration purposes include the functionalities as:

Police Department

- Registration
- Login
- Criminal Records Entry Form
- Evidence upload in IPFS
- Retrieve records when needed (Availability)

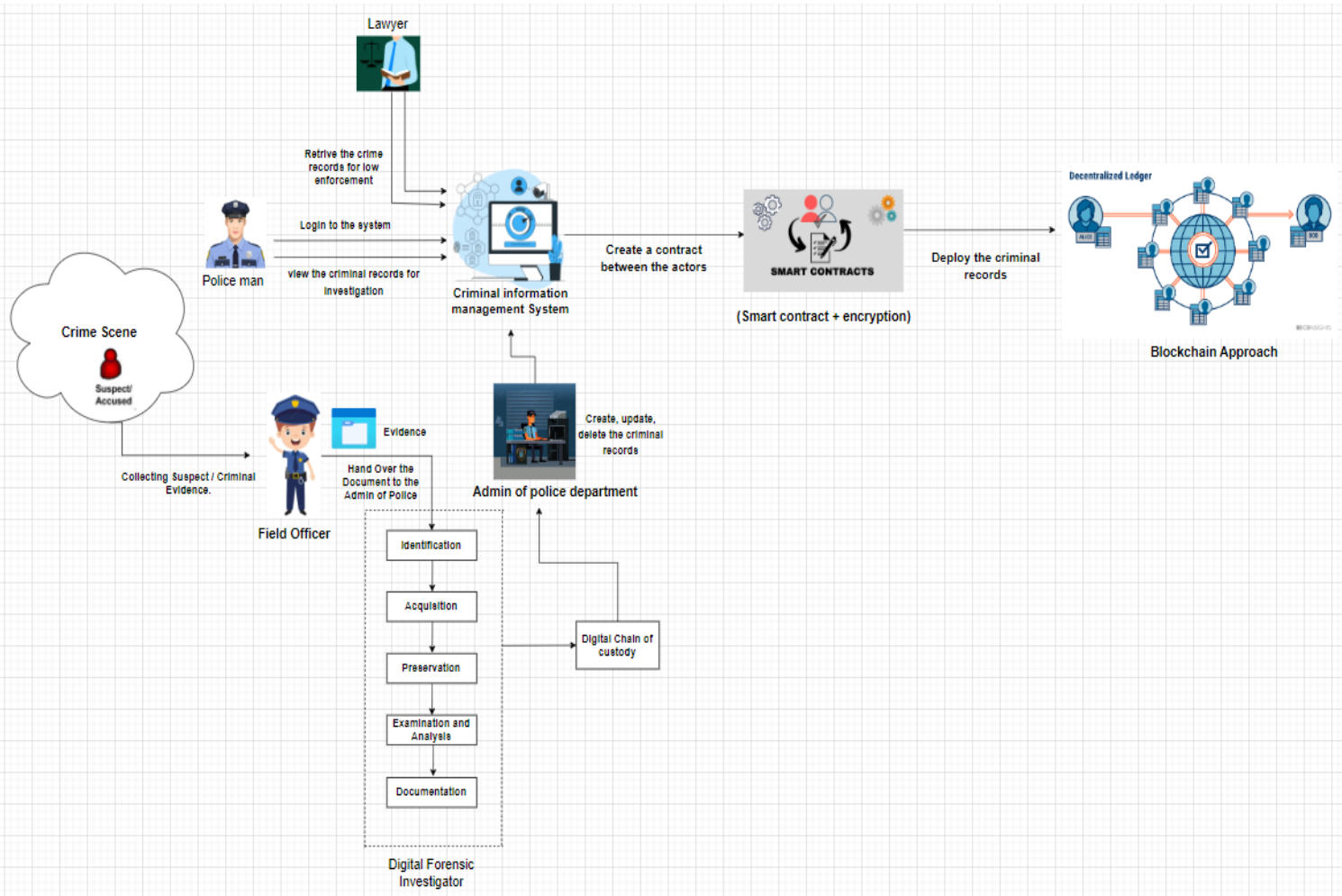


Figure 11:Criminal system with Smart Contracts for blockchain network

2.2.System Overview

The proposed process involves users as Law enforcement authorities as police Officers and Lawyers. In the context of Sri Lanka's criminal justice system, we are faced with challenges stemming from outdated information management methods. The existing system relies heavily on localized databases and paper records, leading to inefficiencies and security concerns. To address these issues, we propose the implementation of a Blockchain-based Criminal Information Management System. In this envisioned solution, we recognize that the Sri Lankan police department, like many other institutions, faces limitations in adopting blockchain technology directly. These constraints include a lack of infrastructure, limited knowledge, and financial constraints. Therefore, we suggest a progressive approach to enhance the system's efficiency and reliability.

Our proposed blockchain-based criminal information management system (CIMS) aims to revolutionize how criminal data is managed and accessed in Sri Lanka. It provides a secure and tamper-proof platform for the storage and retrieval of critical criminal information. The system will be implemented in a phased approach, beginning with the integration of blockchain technology within beneficiary institutions. These institutions, which include law enforcement, judicial bodies, and correctional facilities, play a crucial role in validating and maintaining criminal records. Smart contracts will then be implemented to automate the validation process and define the rules and logic for updating criminal information. This will ensure that the data stored on the blockchain is accurate and reliable.

As the system matures and the institutions become more familiar with blockchain technology, we envision a broader adoption. The reputation of these institutions as trusted entities in the criminal justice sector will further bolster trust in the system. Donors can fund the project with confidence, knowing that their contributions support a transparent and secure CIMS. Our proposed solution acknowledges the current limitations in adopting blockchain technology in Sri Lanka's criminal justice system. By focusing on beneficiary institutions, gradually implementing blockchain and smart contracts, and leveraging institutional trust, we aim to revolutionize the management of criminal information while ensuring data integrity and security.

Table 4:System Users

System Users	Functionality
Law Enforcement authorities • Admin • Police Officers	• Register • Record Criminal's Data • Crime Information / Inquiry
Lawyers	• Register • View Criminal Records • Update Records
Field Offices	• Register • View Criminal Records • Update Records

Overview of the Criminal information management system application shows an overall solution and how users interact with the system and the blockchain as well as the functionality and interaction of each category of users. Once the criminal records are added by the admin user they can view and retrieve the records in the applications. In the blockchain networks it creates the blocks itself for criminal records that user entered. And it is showing all the logs of the transaction and keep the records more securely.

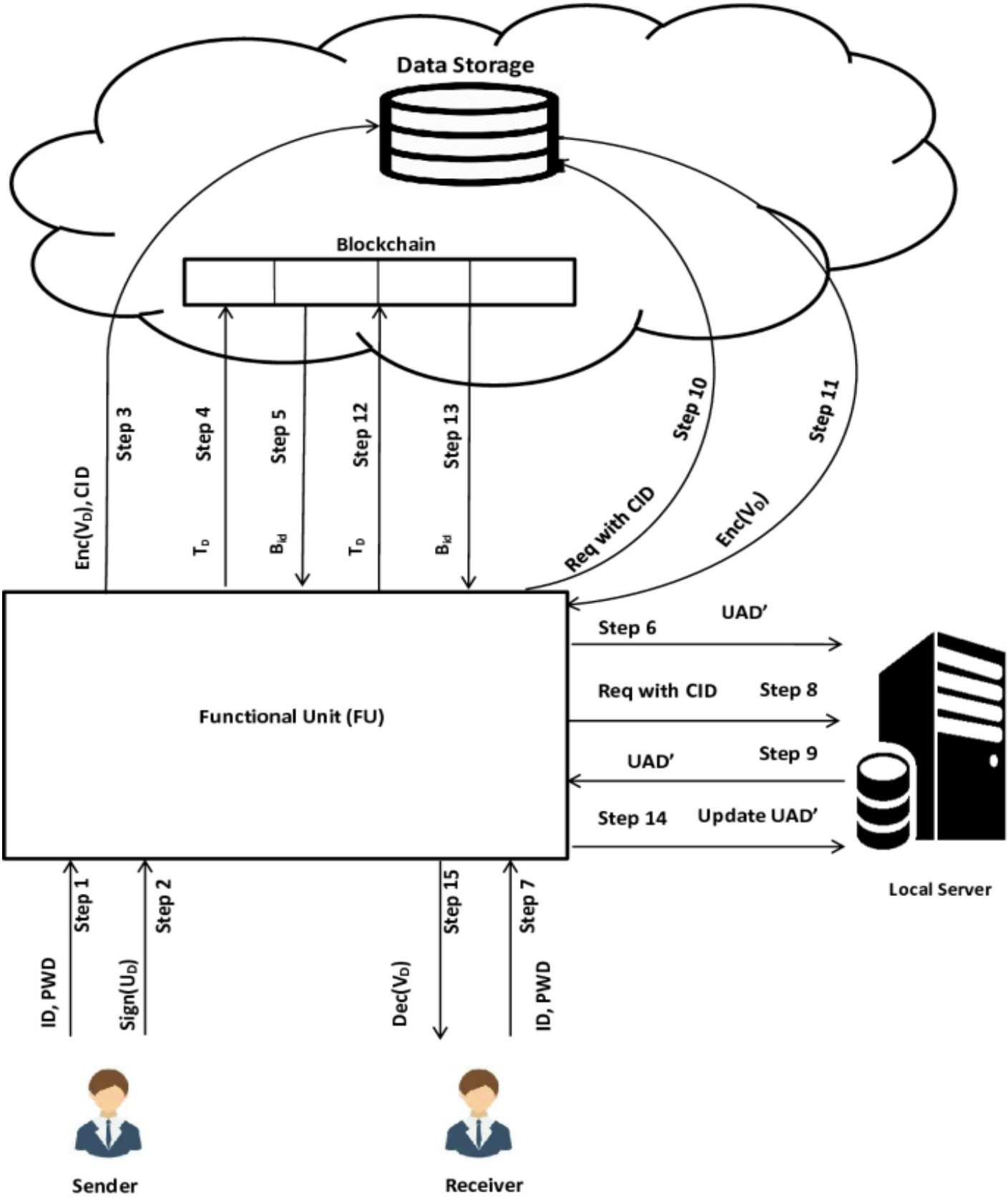


Figure 12:Overview of the Application

2.3.SMART CONTRACT FOR BLOCKCHAIN

In this part, focusing on the criminal information management system is deployed with the blockchain network. Many challenges limit the accuracy and usefulness of Sri Lanka's traditional paper-based criminal information management system. In Sri Lanka, the current criminal information management system relies on traditional paper-based methods. However, this approach proves to be highly time-consuming when it comes to storing, retrieving, and updating criminal records. Relying only on paper records takes a lot of time and increases the danger of data integrity and confidentiality being compromised. As a result, several issues arise, including violations of confidentiality, integrity, and availability, as well as the scattering of criminal data. To tackle this problem, our team proposes adopting a blockchain-based technology for the criminal information management system. Our solution involves the development of a smart contract in blockchain that establishes a connection between the criminal information management system and the blockchain approach. This innovative concept aims to ensure the validation of confidentiality, integrity, and availability of criminal records. Furthermore, it seeks to minimize interoperability problems encountered when identifying criminal records while prioritizing the privacy and security of such sensitive information[10]. Additionally, the dispersed nature of criminal records makes it more challenging for law enforcement organizations to obtain and correlate information effectively. We suggest using blockchain-based technology to implement a remedy to these serious flaws. We seek to transform the criminal information management system by utilizing the decentralized characteristics of blockchain and providing greater security, quicker procedures, and accessibility.

This proposed solution, smart contracts, are designed with Criminal Information Management based on the General Data Protection Regulation [GDPR] Act law enforcement policies & Procedures. The study synthesis was to evaluate smart contracts' current state in relation to the blockchain-based criminal information management system. The investigation was rigorously carried out by carefully going over the readily accessible pertinent material. The creation of specific research questions, the use of relevant databases, and the application of methodical techniques for the identification and assessment of information were all part of the review process. The goal was to present a 3 thorough and transparent evaluation of the function of smart contracts in blockchain technology to administer criminal information [11].

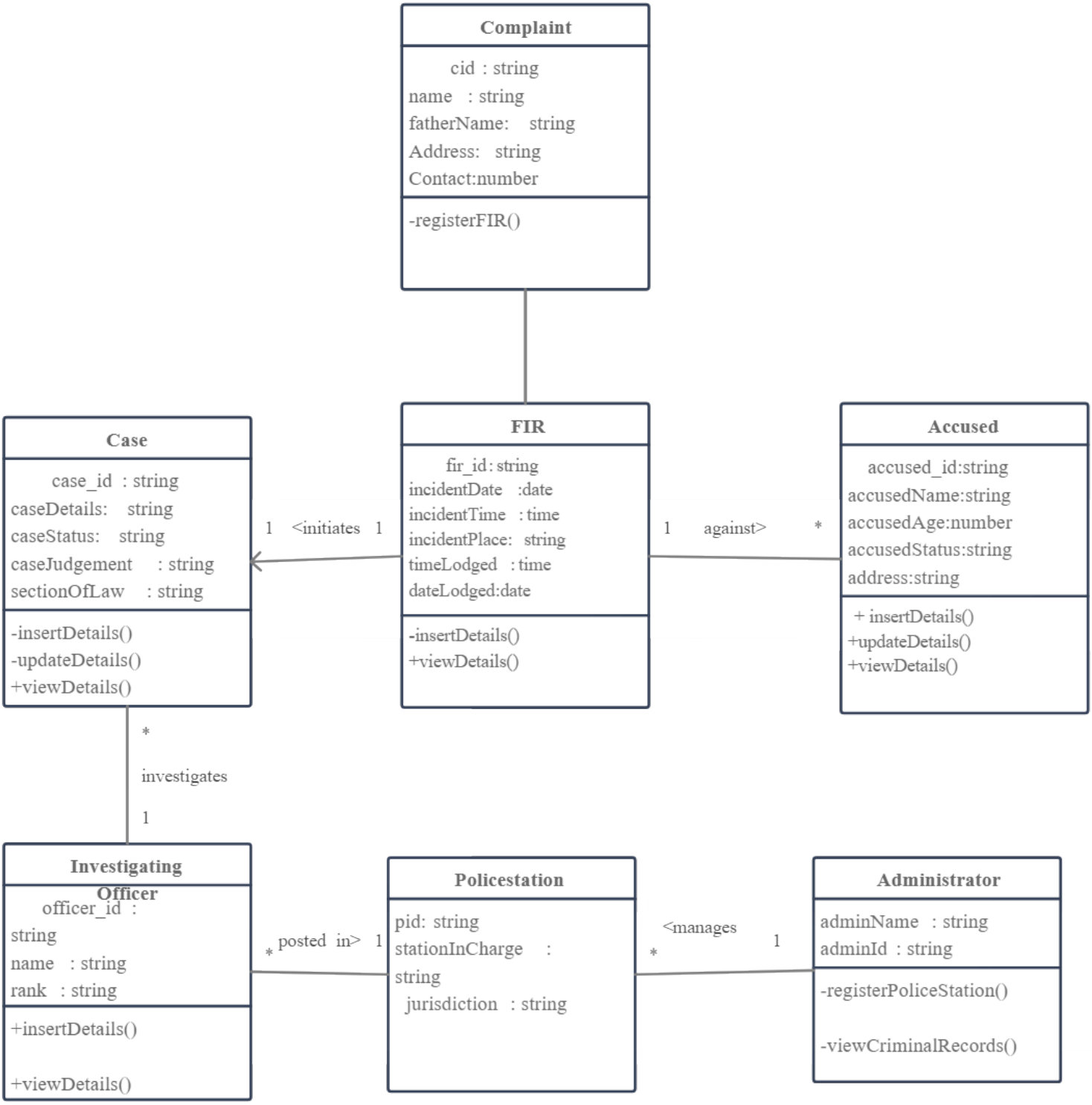


Figure 13:Criminal information management system main functionalities

Criminal information management system main functionalities shows Authorized users will be able to create and update criminal records, including information about individuals, cases, charges, and related details. Validation checks will be implemented to ensure data accuracy and completeness. Powerful search functionality will be provided to allow users to query the database for specific criminal records based on various criteria, such as name, case number, or date. Advanced search filters will be offered to narrow down results.

Users will be able to view the details of criminal records, including case history, charges, court decisions, and associated documents. The option to generate printable versions of records for legal or administrative purposes will be provided. A comprehensive audit trail will be maintained for each record, tracking all changes, updates, and access activities. Authorized users will be able to review the history of any record to maintain transparency and accountability.

Users will be able to attach relevant documents, such as arrest reports, evidence files, and court documents, to criminal records. Document versioning and categorization will be supported. An alert system will be implemented to notify users of critical events related to specific records, such as court dates, warrant issuances, or parole hearings. Users will be able to customize notification preferences. The CIMS will facilitate secure data sharing among authorized users and departments within the criminal justice system. It will support collaboration on cases and investigations, allowing for notes and comments. Tools for generating comprehensive reports and exporting data in various formats, including PDF, CSV, or Excel, will be provided. Custom report generation based on user-defined criteria will be supported.

Robust security measures will be implemented to protect sensitive criminal records from unauthorized access or data breaches. Access control settings and user permissions will be regularly reviewed and updated. Compliance with data privacy laws and regulations, especially regarding the handling of personally identifiable information (PII) and sensitive data, will be ensured. Data anonymization or pseudonymization will be implemented where applicable.

The CIMS will allow seamless integration with other systems used in the criminal justice ecosystem, such as court management systems, law enforcement databases, and correctional facility records. Training sessions and user support will be offered to help users effectively navigate and utilize the CRMS. Documentation and help resources will be provided.

Regular data backup procedures will be implemented to prevent data loss in the event of system failures or emergencies. Reliable data recovery mechanisms will be ensured. Customizable

dashboards and analytics tools will be offered to users to gain insights into trends, case loads, and system performance.

2.4. Software architecture

In the quest to design, develop, and implement a Blockchain-Based Criminal Information Management System (CIMS) for Sri Lanka, our research journey has been marked by a commitment to innovation and adaptability. At the heart of this endeavor lies the meticulous orchestration of the system development process, a journey guided by the principles of agility and responsiveness. In recognition of the dynamic and evolving landscape of criminal information management, we chose to adopt the Agile Software Development Methodology - a nimble and iterative approach that prioritizes collaboration, flexibility, and the continuous refinement of the system. Figure 14, will provide an explanation of the development process.

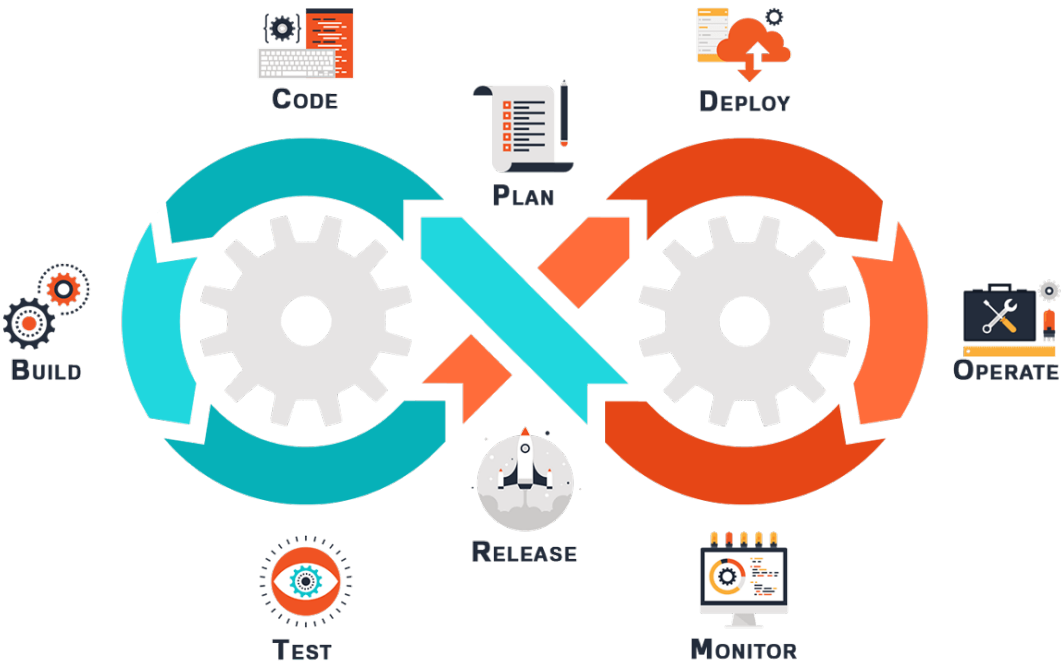


Figure 14:Agile software Development Methodology

2.5. Framework for Innovation and Adaptation

The Agile Software Development Methodology, renowned for its versatility and iterative nature, has played a pivotal role in shaping the development of our blockchain-based CIMS. Unlike traditional, linear development approaches, Agile places a premium on close collaboration among cross-functional teams, frequent reassessment of project goals, and the seamless integration of feedback from end-users. This methodology aligns harmoniously with the ever-changing dynamics of criminal information management, enabling us to respond swiftly to emerging requirements and challenges.

2.6.Iterative Progress: The Agile Advantage

Within the context of our research, the Agile approach has manifested as a series of iterative cycles, each designed to build upon the previous one. These iterations have enabled us to continuously refine our system, incorporating new features, addressing potential issues, and ensuring that the product aligns seamlessly with the evolving needs of law enforcement agencies, the judiciary, and the citizens of Sri Lanka. By breaking down the development process into manageable increments, Agile has allowed us to strike a delicate balance between innovation and adaptability.

In the forthcoming sections, we delve into the specifics of our Agile-based system development process, providing insight into our collaborative workflows, user stories, and sprint cycles. We also explore the unique challenges and advantages that arose as a result of this methodology's application in the development of our blockchain-based CIMS, shedding light on how Agile principles fostered innovation and responsiveness throughout the journey.

Project managers adopted Scrum as a straightforward Agile development methodology to manage a range of iterative and incremental projects. Here, the product owner will create a product backlog using Scrum, and the development team will then find and rank system features in accordance [8].

2.7.Front-end Implementation

The web page refers to the implementation of user's interface where the application users interact with the system to enter criminal records in the web application, view, and update (if required). The interfaces need to be simple, self-explanatory, and easy to use since the police departments and low enforcements authorities like lawyers are asked to register themselves, React JS, JS are used for front-end implementation while react framework is used to ensure clarity and attractiveness of the front-end

The Law enforcement authorities can register and use this system. Admin can manage the criminal records using this system. It ensure the confidentiality, integrity, and availability of the data, because of using the blockchain technology.

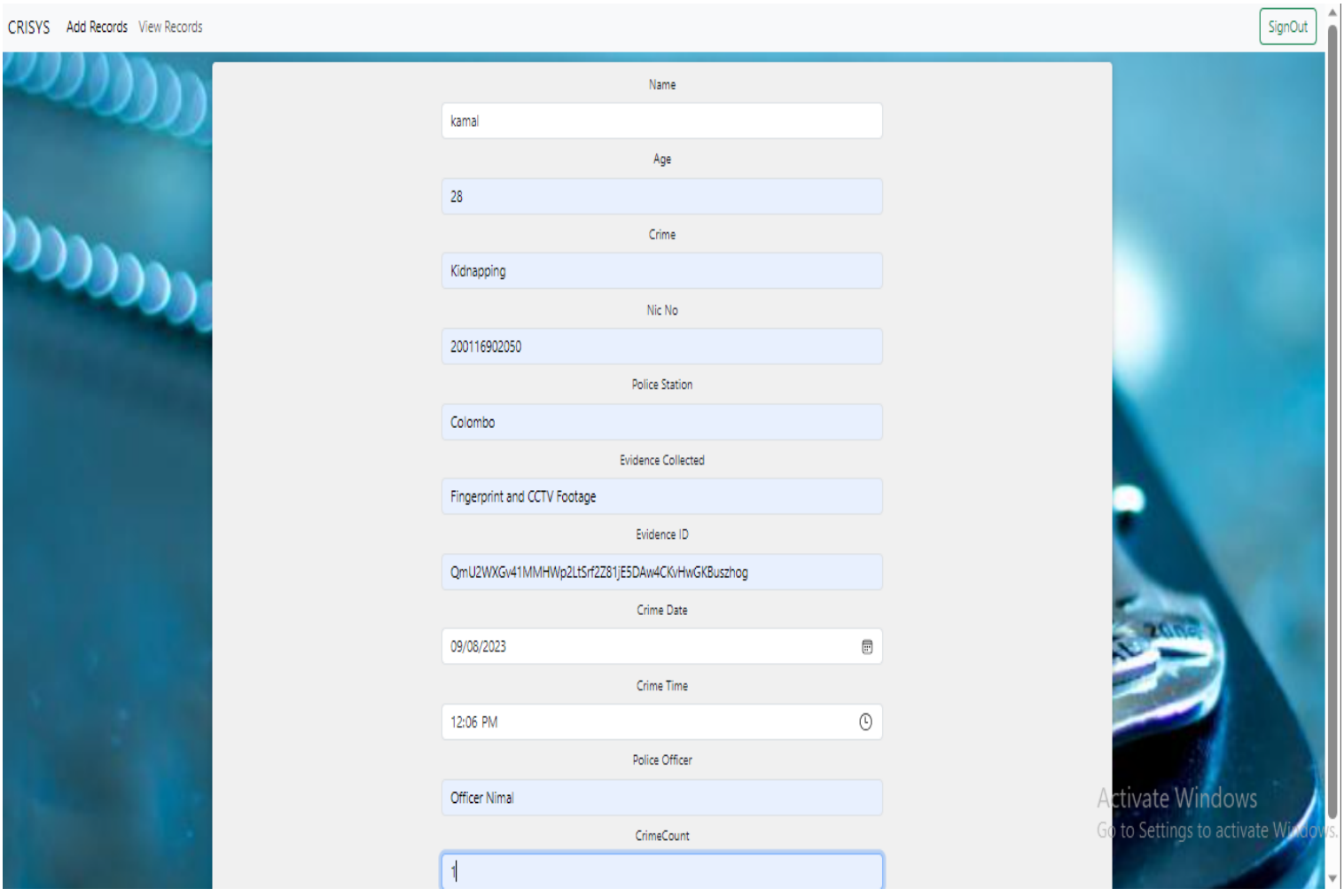


Figure 15:Criminal Records Entry Form

Figure 16:Criminal Records Retrieve Form web page.

2.8.File Validation

Authorized parties can add supporting documents to their case records in a blockchain-based criminal information management system. Critical evidence elements, such as witness statements, forensic findings, or legal documents, issued by pertinent authorities, may be included in these documents. These files are safely uploaded to a web server, where they are kept.

Each file is given a cryptographic hash that is calculated and stored on the blockchain together with the relevant case information to guarantee the consistency and legitimacy of these documents. The facts about the case and the supporting papers are linked securely and permanently through this process. To ensure that the original documents haven't been changed or tampered with in any way, the system automatically validates the file hash whenever these papers are downloaded for review by authorized parties.

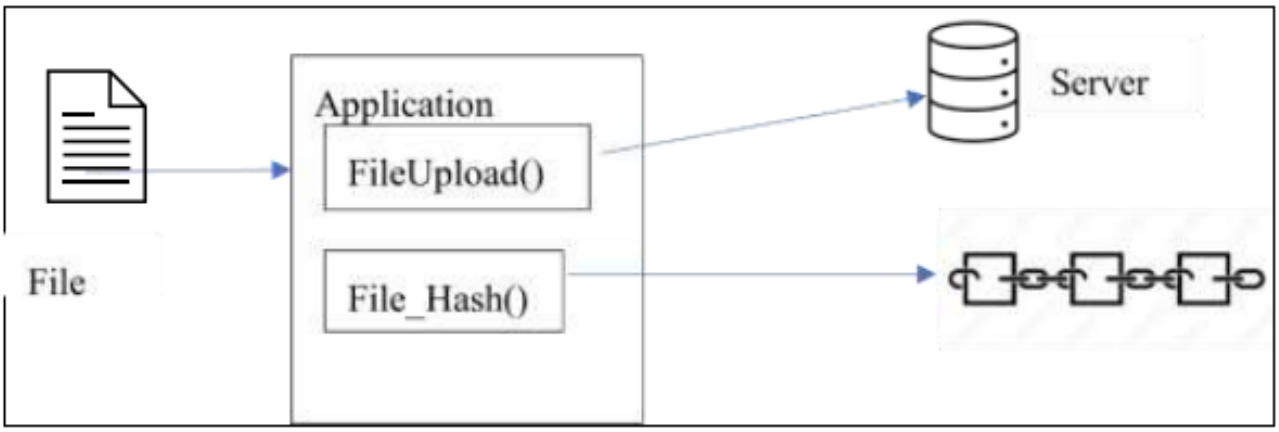


Figure 18:File upload and Hashing process.

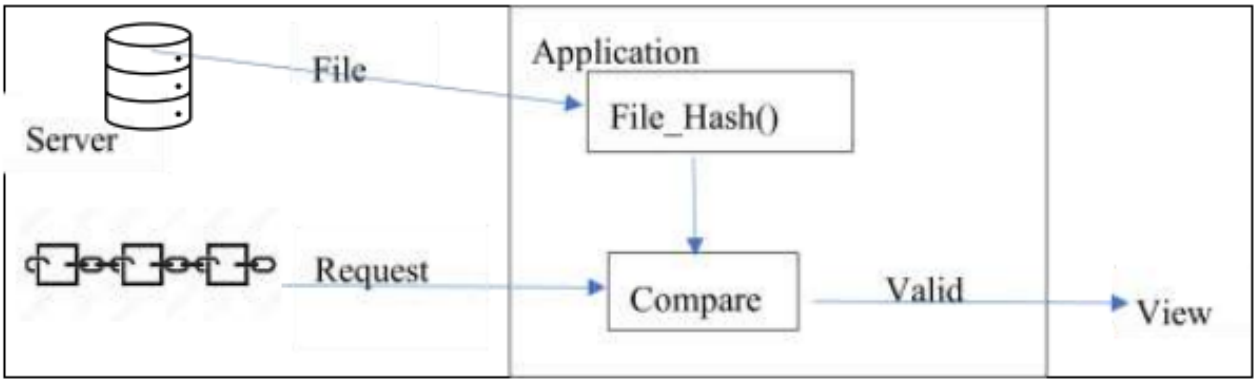


Figure 17:File Validation

The Blockchain-Based Criminal Information Management System is a system that everyone within a country should have access to. Civilians will have the opportunity to report incidents and crimes that they have witnessed. The Blockchain-Based Criminal Information Management System will need to have different login privileges; for example, the privileges that a civilian should have is to report a crime, police officers should be able to report crimes, look into crime folders, investigate through the documentation, etc.

The authentication system that was proposed will be implemented no matter the login privilege the user has. Additionally, since this is an authentication system and can be implemented separately, this system can be used by other systems, applications, and software. So, if the targeted audience were listed for this authentication system, it would be as the following.

- Blockchain-Based Criminal Information Management System Users
    - Civilience
    - Law Enforcement
    - Police Officers
- Social Media Applications
- Hospitals
- Police Departments
- Vulnerability Scanning Tools
    - Example: Acunetix
- Cyber Security Monitoring Tools
    - Example: CrowdStrike

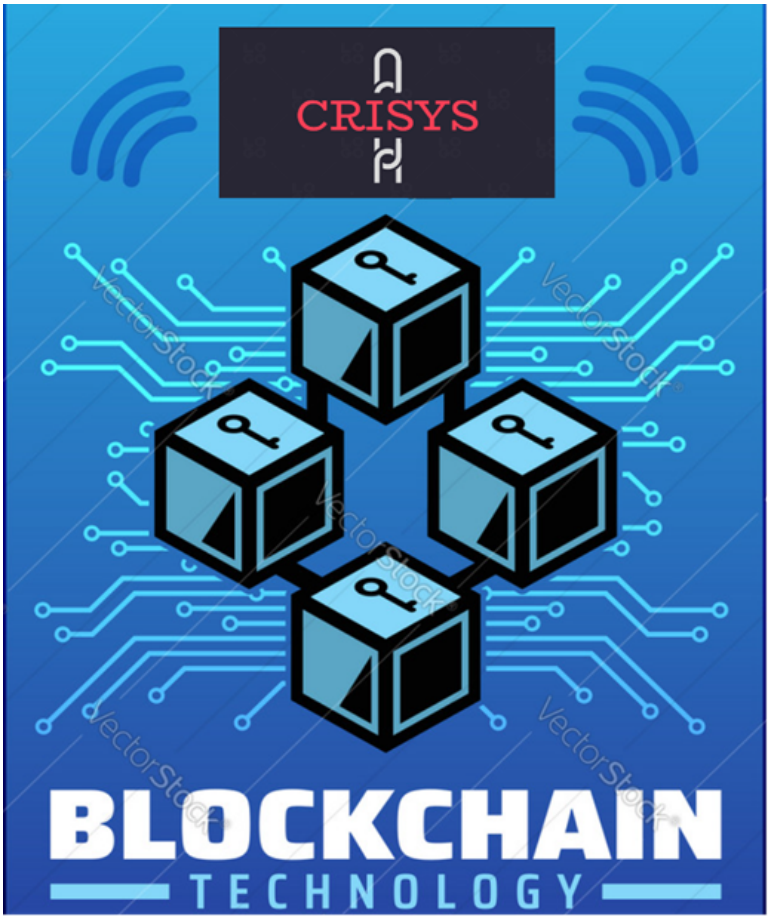


Figure 19:Commercialization Poster

2.10. Testing and Implementation

The Criminal information management system based on blockchain technology tested on Ganache personal Blockchain and MetaMask wallet. It deployed with the Criminal System and tested on blockchain environment. In smart Contracts implementation the application front-end accessed via browsers. The application needs to send data to the blockchain through smart contracts after verifying and validating.

Smart contracts implement functions for request validation and profile maintenance. Encrypted Criminal Records, Crime information, evidence management system and registration details of law enforcement agencies are stored in structs and accessed with mappings on Blockchain. The Confidential information once saved are unchangeable and added via validations through smart contracts.

Home criminal_information.sol

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract CriminalInformation {
    struct CriminalRecord {
        string criminalName;
        uint256 age;
        string crime;
        string nicNo;
        string policeStation;
        string evidenceCollected;
        string evidenceId;
        string crimeDate;
        string crimeTime;
        string policeOfficer;
        uint256 crimeCount;
    }

    mapping(uint256 => CriminalRecord) private criminalRecords;
    uint256 private recordCount;

    event RecordAdded(
        uint256 indexed recordId,
        string criminalName,
```

Figure 21:Data Structure of Solidity

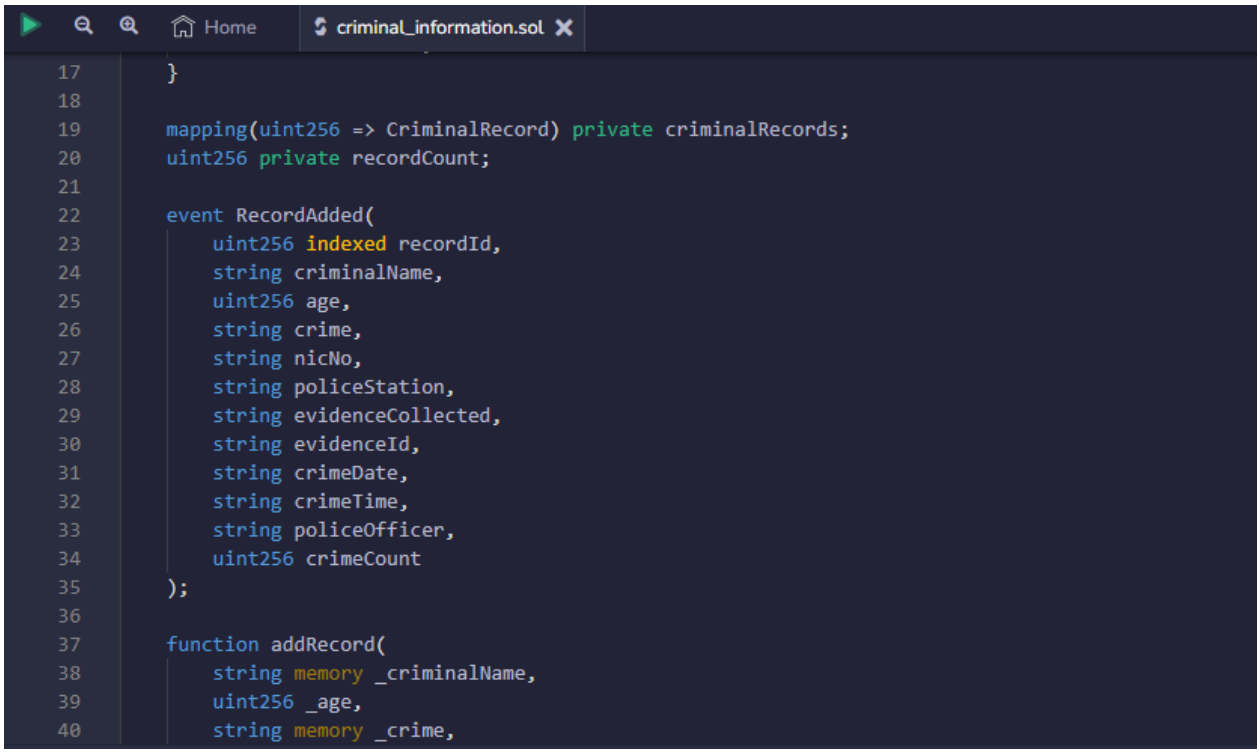


Figure 20:Data structure of Record Added function.

Solidity Code for Smart Contract deploy with Blockchain.

```
// SPDX-License-Identifier: MIT

pragma solidity ^0.8.0;


contract CriminalInformation {
    struct CriminalRecord {
        string criminalName;
        uint256 age;
        string crime;
        string nicNo;
        string policeStation;
        string evidenceCollected;
        string evidenceId;
        string crimeDate;
        string crimeTime;
        string policeOfficer;
        uint256 crimeCount;
    }

    mapping(uint256 => CriminalRecord) private criminalRecords;
    uint256 private recordCount;
```

Input fields of the Criminal Entry Form

Using struct function and the relevant data structure.

```
event RecordAdded(
    uint256 indexed recordId,
    string criminalName,
    uint256 age,
    string crime,
    string nicNo,
    string policeStation,
    string evidenceCollected,
    string evidenceId,
    string crimeDate,
    string crimeTime,
    string policeOfficer,
    uint256 crimeCount
);
```

View Records Function of Criminal Records

Once we entered the records in add record option can show the added records

```
function addRecord(
    string memory _criminalName,
    uint256 _age,
    string memory _crime,
    string memory _nicNo,
    string memory _policeStation,
    string memory _evidenceCollected,
    string memory _evidenceId,
    string memory _crimeDate,
    string memory _crimeTime,
```

Add Records Function of Criminal Records

Once user entered the records in add record tab

```
    string memory _policeOfficer,
    uint256 _crimeCount
) public {
    require(bytes(_criminalName).length > 0, "Criminal Name must not be empty");
    require(_age > 0, "Age must be greater than zero");
    require(bytes(_crime).length > 0, "Crime must not be empty");
    require(bytes(_nicNo).length > 0, "NIC No must not be empty");
    require(bytes(_policeStation).length > 0, "Police Station must not be empty");

    recordCount++;
    criminalRecords[recordCount] = CriminalRecord(
        _criminalName,
        _age,
        _crime,
        _nicNo,
        _policeStation,
        _evidenceCollected,
        _evidenceId,
        _crimeDate,
        _crimeTime,
        _policeOfficer,
        _crimeCount
    );
    emit RecordAdded(
```

Condition added in the input fields

Counting each record for security concerns and all the entered records have a unique id

```
        recordCount,
        _criminalName,
        _age,
        _crime,
        _nicNo,
        _policeStation,
        _evidenceCollected,
        _evidenceId,
        _crimeDate,
        _crimeTime,
        _policeOfficer,
        _crimeCount
    );
}

function getRecord(uint256 _recordId)
    public
    view
    returns (
        string memory criminalName,
        uint256 age,
        string memory crime,
        string memory nicNo,
        string memory policeStation,
```

```
        string memory evidenceCollected,
        string memory evidenceId,
        string memory crimeDate,
        string memory crimeTime,
        string memory policeOfficer,
        uint256 crimeCount
    )
{
    require(_recordId > 0 && _recordId <= recordCount, "Invalid record ID");

    CriminalRecord memory record = criminalRecords[_recordId];
    return (
        record.criminalName,
        record.age,
        record.crime,
        record.nicNo,
        record.policeStation,
        record.evidenceCollected,
        record.evidenceId,
        record.crimeDate,
        record.crimeTime,
        record.policeOfficer,
        record.crimeCount
    );
```

Retrieve Records function

```
    }

    function getTotalRecords() public view returns (uint256) {
        return recordCount;
    }
}
```

The user-facing frontend of the application plays a crucial role in collecting user inputs and initiating requests to the smart contracts for assessment. To ensure secure and authenticated transactions, a dedicated wallet system is employed, responsible for transaction verification and communication with the relevant blockchain network.

In this ecosystem, a specialized JavaScript library known as Web3.js assumes the responsibility of facilitating interactions with the Ethereum node. Web3.js offers versatile communication options, including HTTP, IPC, or WebSocket, and provides a user-friendly API for seamless JSON-RPC communication. By utilizing this library, developers of decentralized applications (Dapps) can streamline the process of executing RPC calls, reducing the complexity of the coding task. Furthermore, the Web3.js library can be accessed either from its original source location or installed locally, providing flexibility and convenience for developers.

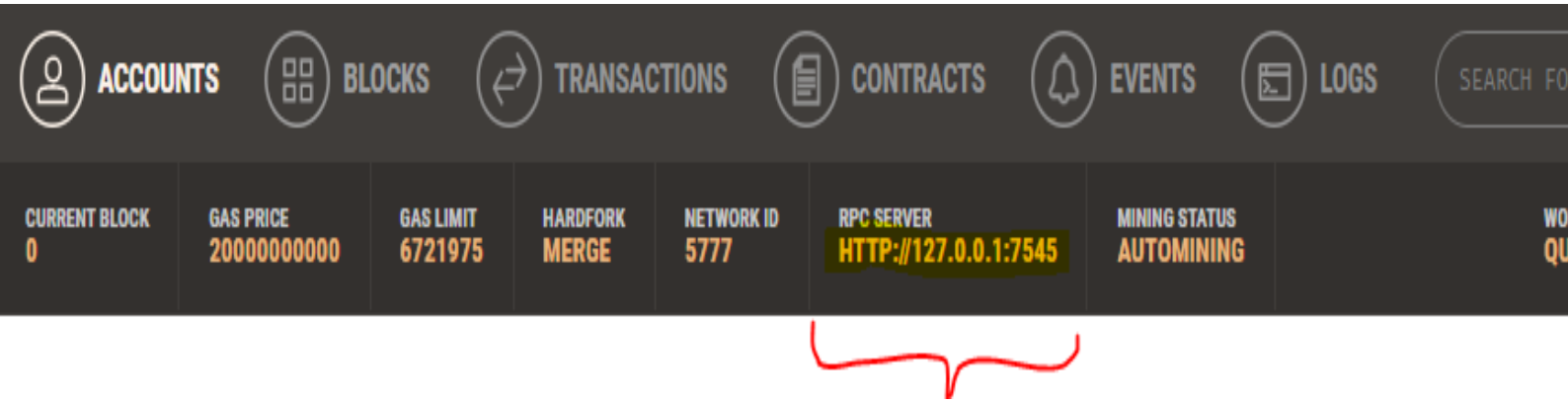


Figure 22:Blockchain Network running on RPC server.

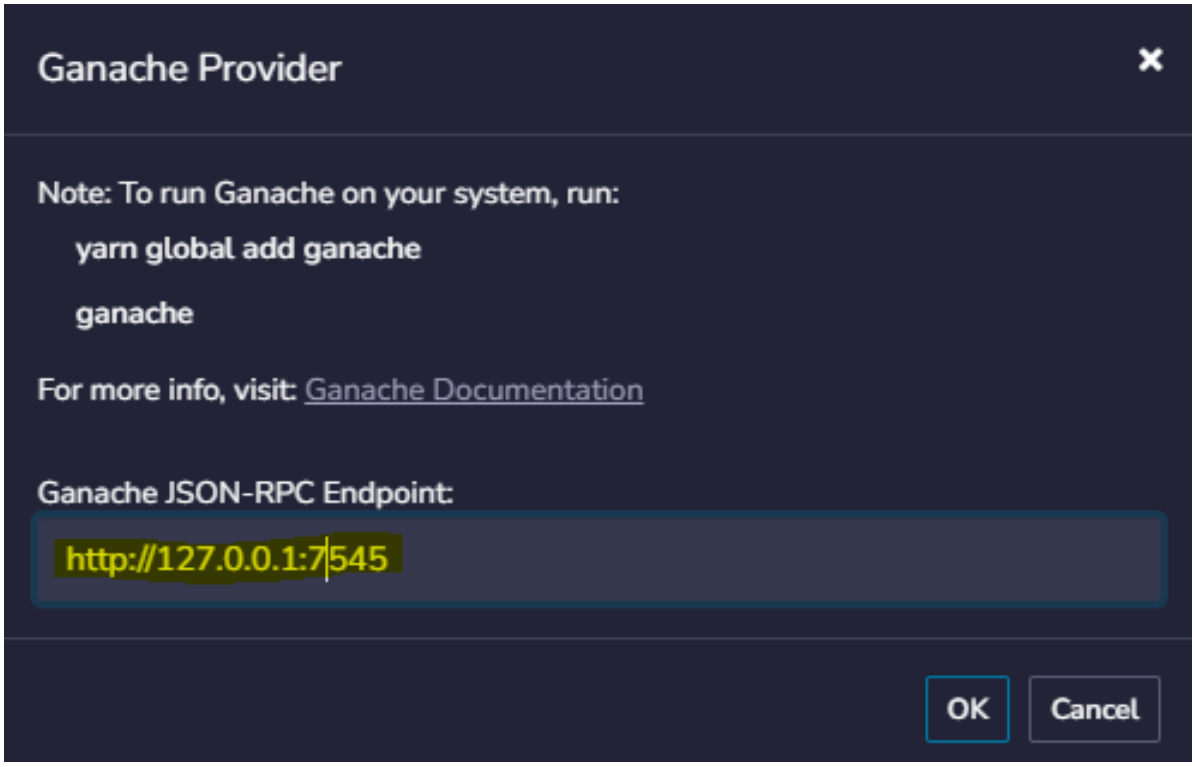


Figure 23:Connect with solidity code.

working product testing

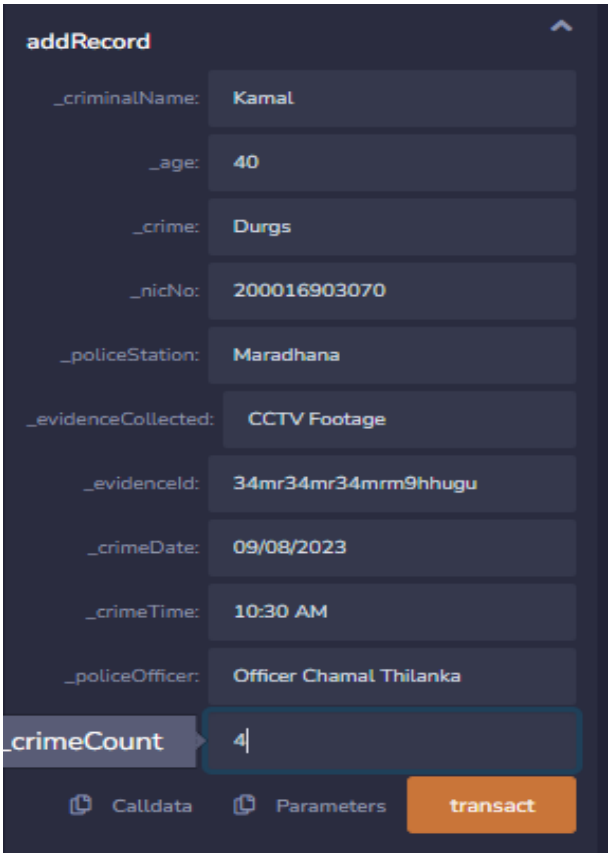


Figure 25:Add record interface.

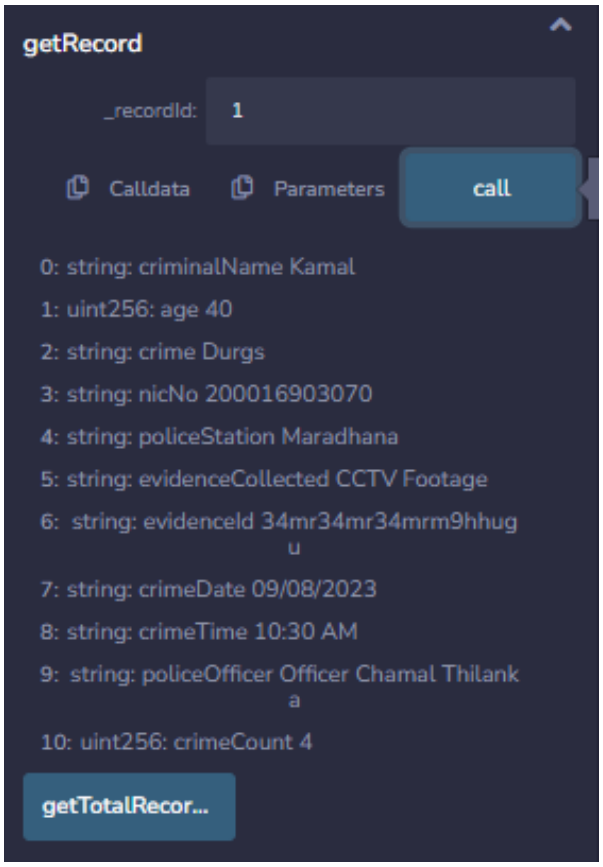


Figure 24:Get record function on interface.

Figure 27:Transaction for each record deploy with the block details and Gas wastage.

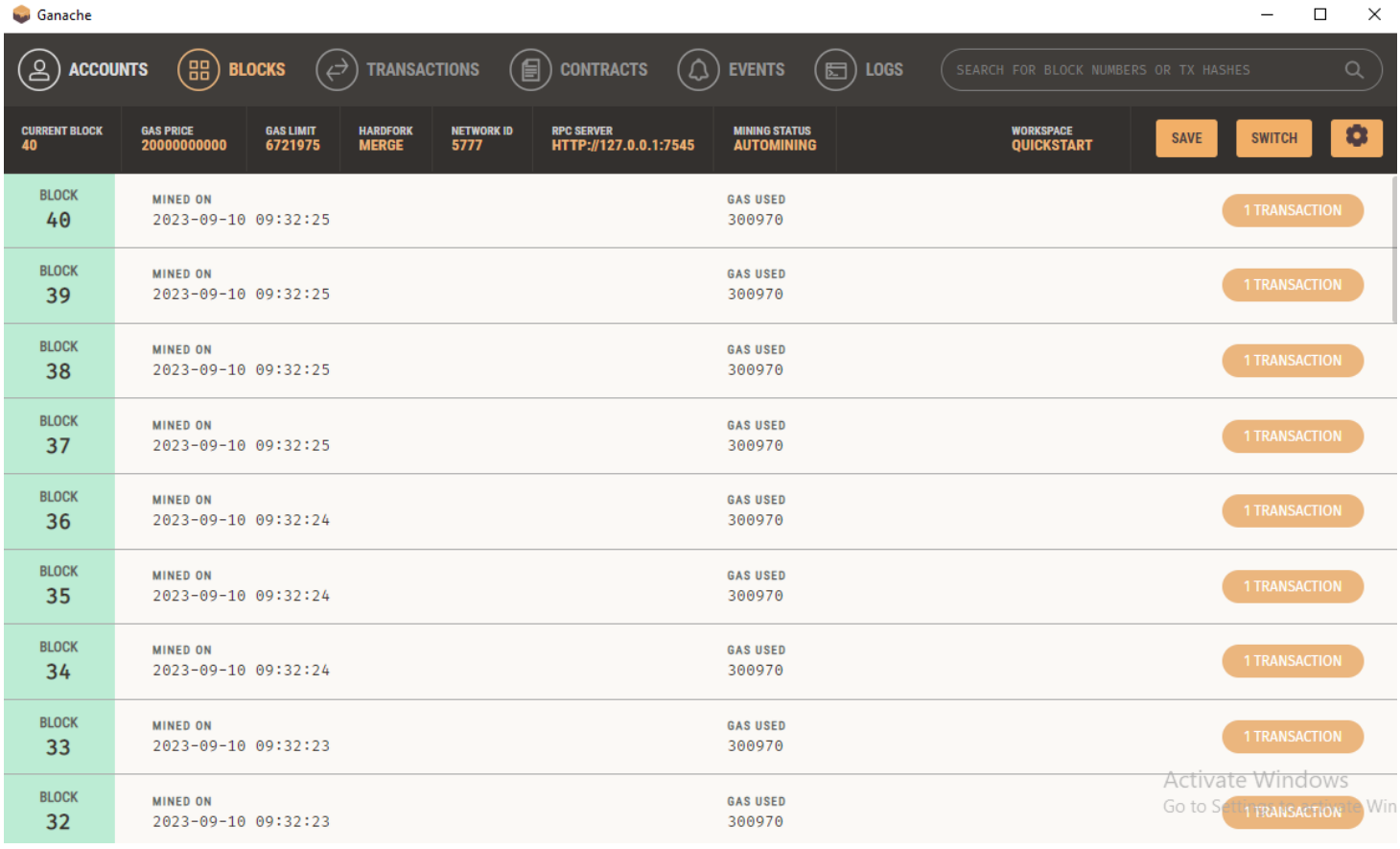


Figure 26:Tested the records on blockchain.

related users. Inside the block it is stored as hash value, and we can't reverse it back. Each block contains Contract address, from address, gas used for the transaction and the block of the hash will return to user. The blockchain only stored text-based information.

If we visualize the Block it look like below picture :

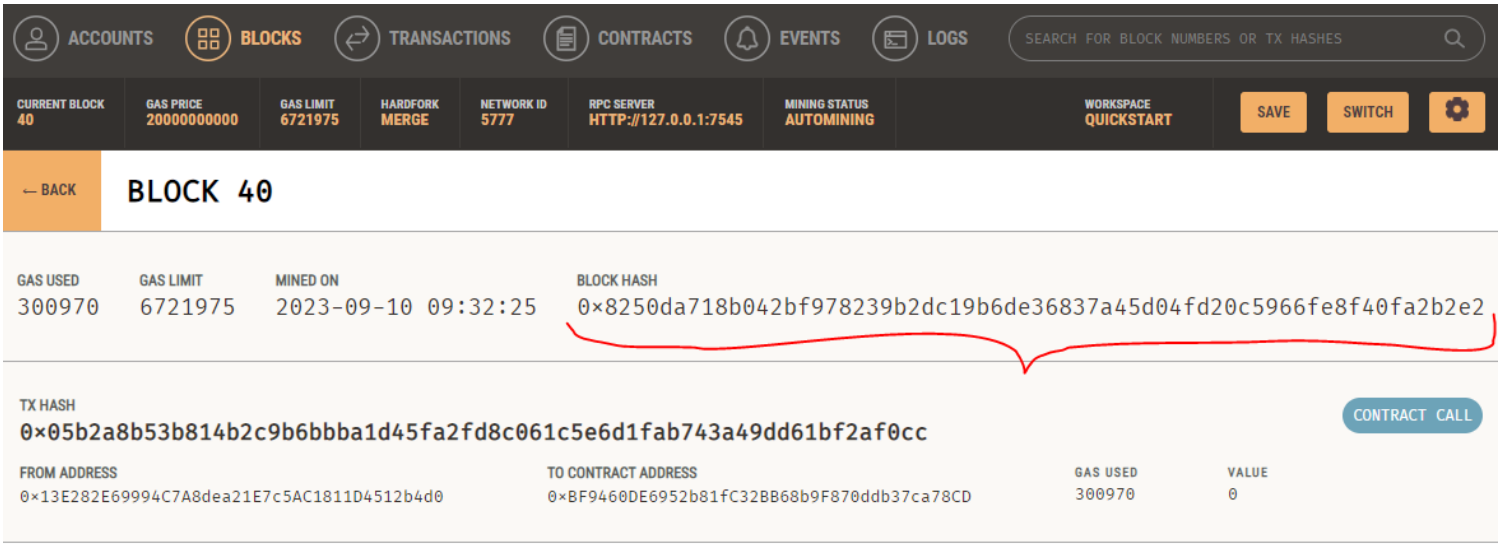


Figure 28:Inside the Block View

Truffle framework is a blockchain application development environment for Ethereum dApp developments. The built-in support for smart contract compiling, linking, deployment and testing is a useful measure implemented. Truffle framework's unique features include.

1. Smart contract management
2. Automated contract testing
3. Scriptable, migration and deployment
4. Network management
5. Interactive console

Ganache, offered by Truffle, serves as a valuable tool within the Ethereum development ecosystem, functioning as a local blockchain and Ethereum simulator. This Integrated Development Environment (IDE) enjoys widespread popularity among developers for Ethereum blockchains.

Ganache fulfills a critical role by providing a test environment that operates locally and virtually, enabling rapid and efficient testing of smart contracts. In the realm of smart contract deployment, migration, and access options, Truffle stands out for its user-friendly approach, simplifying the processes of compilation and deployment while offering enhanced visibility and control over the Ethereum Virtual Machine (EVM).

Developing and testing applications and smart contracts on authentic blockchain networks can be resource-intensive in terms of both costs and time. Deploying contracts on real blockchains entails the expenditure of gas fees, making it a costly endeavor. Moreover, the process of deploying a smart contract on a genuine blockchain can be time-consuming. Therefore, it is often recommended, particularly for research and prototyping purposes, to leverage a local blockchain for testing. Doing so minimizes costs and accelerates the development and testing phases, providing a more efficient environment for experimentation.

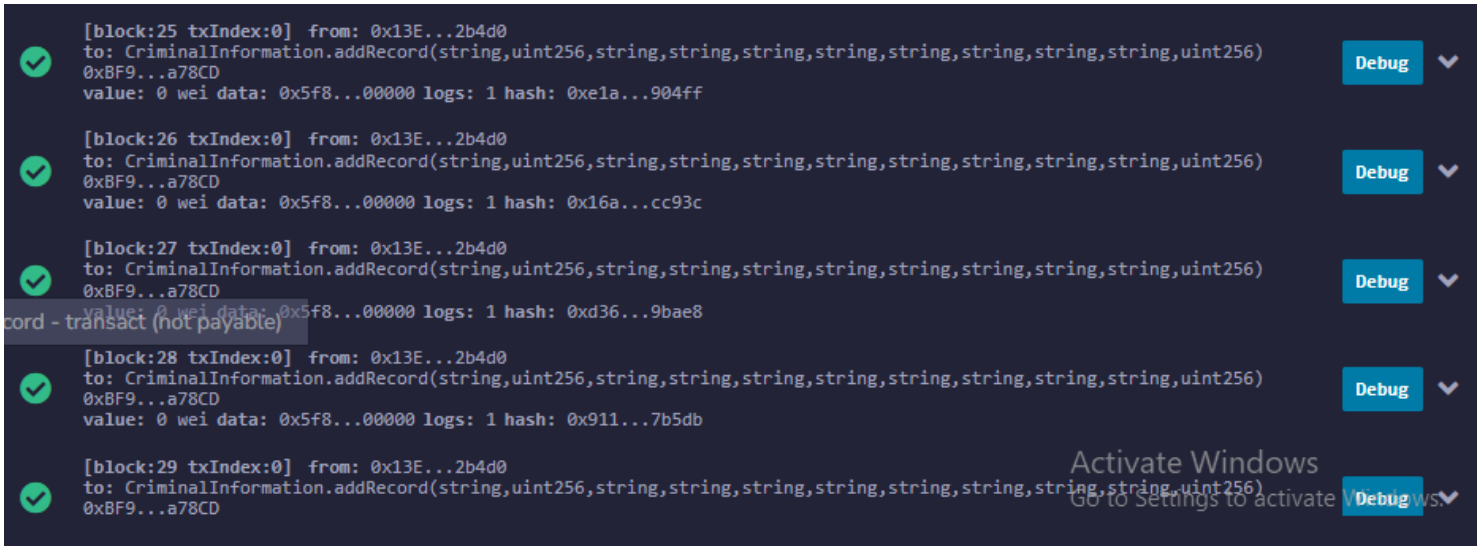


Figure 30:Deploy History of criminal records.

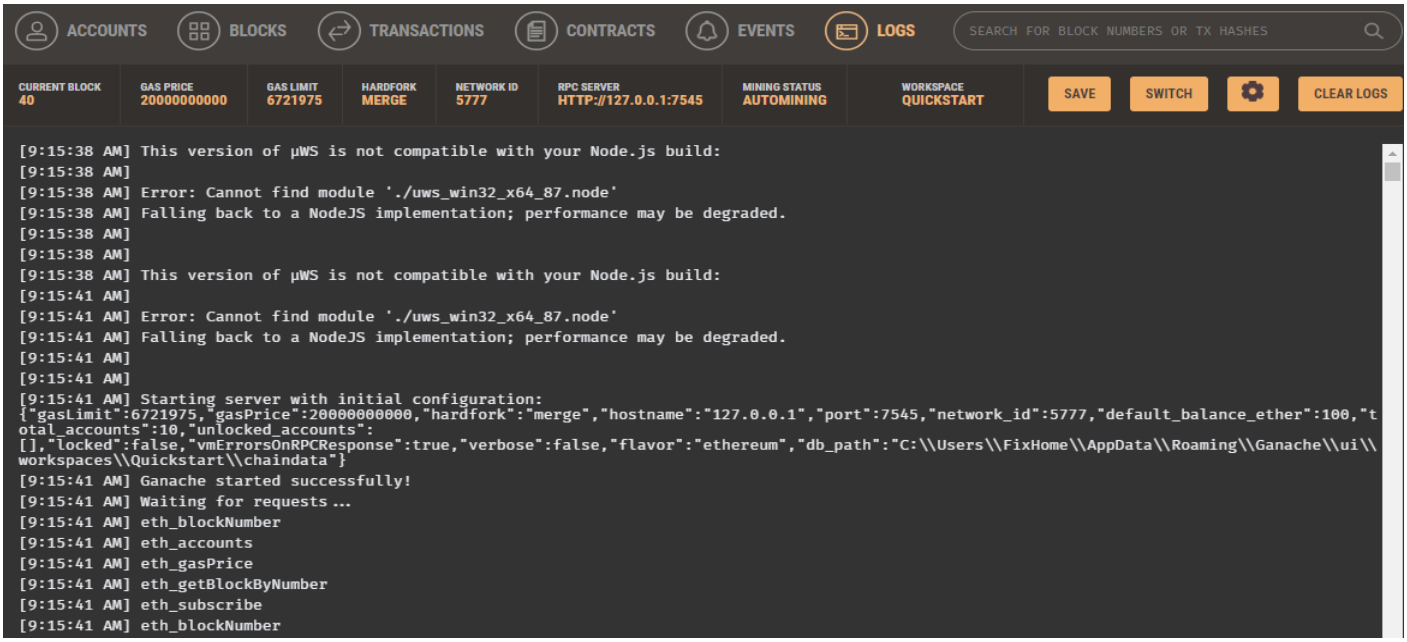


Figure 29:Logs collector for deployed contracts

3. Results and Discussions

The software solution designed for the Blockchain-based criminal information management system requires comprehensive evaluation by a range of stakeholders, including developers, testers, and potential users. In the initial stages of our research, it became evident that establishing trustworthiness was a fundamental requirement. However, the precise definition and understanding of trust within the context of information solutions were not well-defined.

The emergence of blockchain technology has presented a promising avenue for addressing this trust deficit. Globally, there is a growing body of research exploring the concepts of trust and privacy within blockchain-based systems. While these concepts have gained traction in academic and research circles, they have yet to achieve widespread recognition among the public, particularly within the Sri Lankan context.

The concept of cryptocurrency or virtual currency, which is closely tied to blockchain technology, has gained acceptance in many countries. In Sri Lanka, there is a burgeoning interest in virtual currencies, especially among the younger population. However, it is important to note that the lack of endorsement by the Sri Lankan Central Bank has posed a challenge to fostering trust in blockchain-based solutions within the country [35].

These considerations underscore the need for rigorous evaluation, education, and awareness-building efforts when implementing a blockchain-based criminal information management system in Sri Lanka. Building trust and confidence in the technology among stakeholders, including potential donors, is pivotal to the successful adoption of such innovative solutions

3.1.Results

3.1.1. Software testing

The testing and evaluation process for the proposed Blockchain-based criminal information management system is structured around predefined use cases derived from the initial requirement gathering phase. These use cases encompass critical functionalities such as initiating a criminal information request, validating the request (both positive and negative outcomes), approving donations, and updating donor information. To effectively evaluate the system, a set of well-defined test cases has been established. These test cases are specifically

designed to assess the identified features outlined in the solution. Below are some notable test cases:

- Entity Registration: This initial set of test cases focuses on registering system entities, including law enforcement agencies, individuals involved in criminal cases, and authorized users. The successful execution of these test cases demonstrates the system's functionality and its ability to handle entity registration effectively.
- Data Integrity and Usability: The system undergoes extensive testing with sample data to ensure data integrity and usability. The goal is to evaluate the suitability of blockchain technology in preserving the integrity of criminal information and its usability for the application's users.
- Authentication and Authorization: Test cases are devised to evaluate the authentication and authorization mechanisms within the system. This ensures that only authorized users can access and modify criminal information, thereby enhancing security and data confidentiality.
- Criminal Information Requests: The testing process involves simulating criminal information requests and assessing the system's responsiveness in handling such requests. It evaluates whether the system can efficiently process and validate criminal information requests.
- Donation Approval: The system is rigorously tested for its ability to facilitate the approval of donations. This includes verifying whether the system accurately records donation approvals and updates relevant donor information.
- Functional Validation: Throughout the testing phase, the system's functionality is continuously validated to ensure that it consistently performs as expected. This includes confirming that the system meets the predefined use cases and requirements.
- Performance Assessment: Performance testing is conducted to evaluate the system's responsiveness, scalability, and overall performance under various loads and conditions.
- Data Security: The security of criminal information stored on the blockchain is a paramount concern. Test cases are designed to assess data security measures and confirm that sensitive information remains protected from unauthorized access.
- The development testing phase primarily focuses on aligning the system with the identified requirements. Sample data is used for testing, and the system's usability is assessed in the context of criminal information management.

Table 5:Test Cases

ID	Description	activity	Expected Results	Actual Results
B001	Police Department registration	With compulsory information	Success	✓
		Missing compulsory information	Error Message	
B002	Police officer Registration	With mandatory information	Success	✓
		Missing compulsory information	Error Message	
B003	Lawyer Registration	With mandatory information	Success	✓
		Missing compulsory information	Error Message	
B004	Law enforcement agencies access via Web	Correct Credentials	Login success	✓
		Mismatching credentials	Invalid Credential	
B005	Criminal records entry form	Valid information should be added	Record added success	✓
		Invalid Information adding	Invalid Record	
B006	Evidence Management process	Limited access and Encryption protected	Protected	✓

3.2.Smart Contract Testing – Remix IDE

Remix IDE stands as an open-source web application designed to facilitate the development, deployment, and testing of smart contracts on the Ethereum blockchain. It offers an integrated graphical user interface (GUI) that enhances the efficiency and clarity of the testing and learning process for developers. Within Remix IDE, developers can seamlessly write, compile, and deploy smart contracts. Subsequently, they can interact with these contracts by providing the required inputs to the blockchain through the smart contract functions and retrieving information using the same methods. Figure 4.1 provides an illustrative representation of the smart contract testing process within Remix IDE. The assessment of blockchain functionality can be quantified by measuring the gas consumption associated with each transaction and its impact on the Ether (ETH) balance of individual blockchain user accounts. Notably, actions such as recording data on the blockchain incur gas costs, whereas

reading information from the blockchain is gas-free. Furthermore, the Ganache personal blockchain offers valuable insights into each user account's coin balance and transaction-related details. It provides a comprehensive overview of transaction history and associated information.

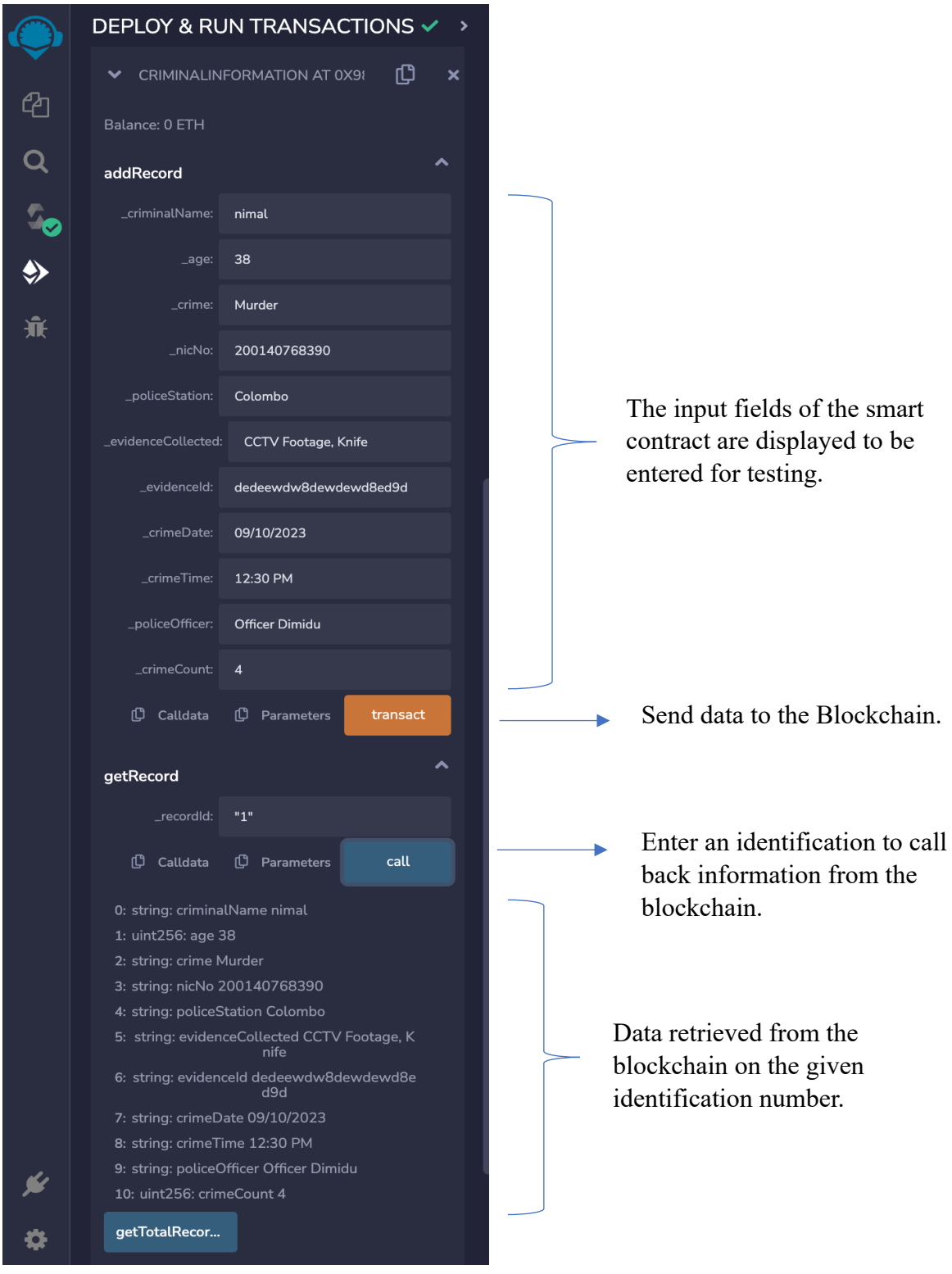
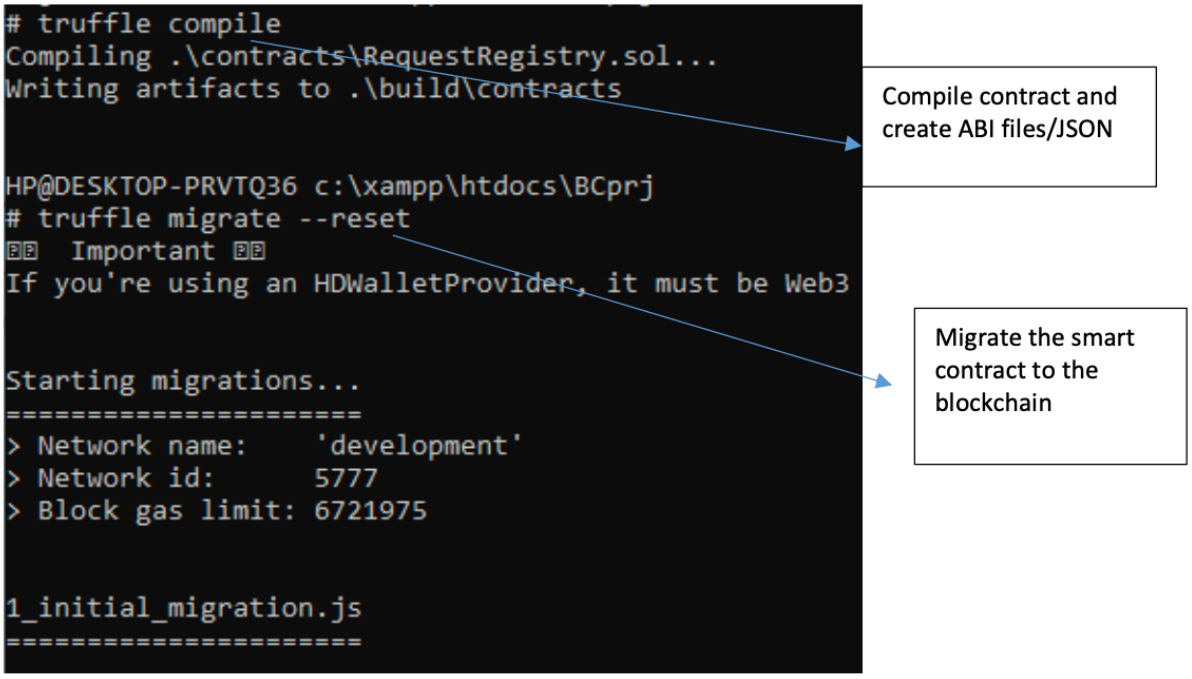


Figure 31:Smart Contracts deployment testing

3.3. Smart Contract Testing – Truffle Console

The smart contract needs to be compiled to create the byte code to be used in the blockchain. And migrated to update the blockchain with the smart contract.




```
# truffle compile
Compiling .\contracts\RequestRegistry.sol...
Writing artifacts to .\build\contracts


HP@DESKTOP-PRVTQ36 c:\xampp\htdocs\BCprj
# truffle migrate --reset
⚠️  Important ⚠️
If you're using an HDWalletProvider, it must be Web3


Starting migrations...
======================
> Network name:    'development'
> Network id:      5777
> Block gas limit: 6721975


1_initial_migration.js
======================
```

Figure 32:Compile and migrate smart contract.

Subsequently, the smart contract is deployed to the blockchain, making it available for data transfers. A deployed smart contract on the blockchain is assigned a unique address, and as it involves a write operation on the blockchain, a corresponding transaction is appended to the blockchain ledger, resulting in a reduction of gas.

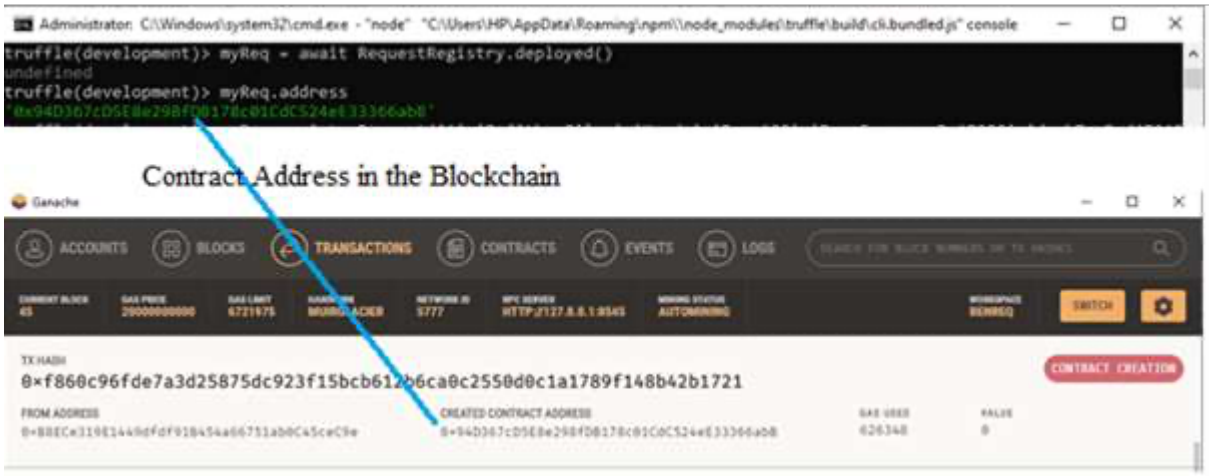


Figure 33:Deploy smart contract to the Blockchain.

Write data to the blockchain via the function registerRequest() in the smart contract. For testing purposes, the function takes arguments as (id, 'Police_Officer_Name', 'Address', 'Registration Number', 'Request Details', 'File Hash').

Security

During the testing phase, the self-verifying and self-enforcing characteristics of smart contracts become evident. These contracts autonomously execute predefined actions when specific conditions are met. For instance, the inclusion of a beneficiary request into the blockchain occurs only when all necessary information is available, and a registered institute initiates a request for a registered beneficiary. Once such a beneficiary request is initiated, the smart contracts deployed on the blockchain automatically self-enforce the defined processes, meticulously verifying and processing the request in accordance with their predetermined logic.

3.4. Discussion

3.4.1. System Security analysis

Integrity:

In the context of the Blockchain-based criminal information management system, data integrity is upheld through the meticulous management of criminal information, which is received through authorized channels and made accessible to relevant parties via the blockchain. Each piece of data is associated with a unique identifier and a transaction ID, ensuring the preservation of data integrity, and enabling the precise identification of every record.

Accountability:

Smart contracts within the system play a pivotal role by assigning distinct identifiers to transactions and facilitating the tracking of criminal information requests. These contracts establish a clear link between the responsible institute initiating the request and the subsequent transaction on the blockchain. This transparency and traceability hold the institute accountable for the requests they submit, fostering authenticity and reliability in their actions.

Authorization and Confidentiality:

Confidentiality and prevention of data forgery are paramount concerns in the realm of criminal information management. Consequently, the system restricts access to beneficiary data exclusively to authorized users. Leveraging the immutability feature inherent in blockchain technology, once transaction details are recorded, they remain unalterable, safeguarding confidentiality and integrity against potential forgery attempts.

Availability:

In a fully deployed blockchain infrastructure, decentralization and distribution are key attributes. Transaction data and accessibility records, once securely stored, are immune to loss or unauthorized alterations. Even in the event of a node failure, unlike centralized solutions, transaction records remain intact, thanks to the decentralized and distributed nature of the blockchain system. This ensures the continuous availability and reliability of critical criminal information, supporting the system's operational resilience.

3.5. Overall Discussion

Permissionless Blockchain:

In the context of the Blockchain-based criminal information management system, the design aligns with the concept of a permissionless blockchain, characterized by its absence of a central governing authority and its open accessibility, which doesn't necessitate permission for users to access and participate in the application. The primary objective of adopting a permissionless approach is to foster inclusivity, encouraging a broader spectrum of institutions to engage and support a diverse array of individuals in need. Furthermore, this approach aims to attract a wide range of police officers, spanning from individuals to organizations. The presence of diverse beneficiaries ensures that even criminals with modest to moderate bad habits can identify suitable cases for their contributions. Additionally, the utilization of a permissionless network eliminates the need for intermediaries, enhancing efficiency and reducing third-party involvement.

However, one potential concern lies in verifying the authenticity of participating institutions. To address this, a more comprehensive solution involves establishing a governing body comprising major law enforcement agencies/authorities. This governing body would oversee the overall management of the application, potentially leading to the transition to a permissioned or private blockchain solution, enhancing security and trustworthiness.

Request Encryption:

Enhancing security measures, users' requests can be encrypted before their inclusion in the blockchain, bolstering the protection of sensitive information. The React framework offers a robust and user-friendly encryption library, employing the AES-256 and AES-128 encryption methods. Additionally, encrypted messages are fortified through Message Authentication Code (MAC) in react JS, effectively preventing unauthorized modifications or interference with encrypted messages.

4. Conclusion

Criminal information management has long grappled with issues of integrity, fraud, and an uneven distribution of resources. Traditional methods of managing criminal data have relied on manual processes or centralized systems, which have often been susceptible to fraudulent activities, scams, and a lack of transparency. The emergence of blockchain technology has introduced a promising paradigm shift, offering attributes such as immutability, decentralized public ledgers, consensus mechanisms, unanimous decision-making, and smart contract automation. These features make blockchain an ideal candidate for enhancing the management of criminal information.

Extensive research, as highlighted in the literature review, has explored the application of blockchain in the realm of criminal information management, particularly in the domains of funding and resource allocation. Notably, blockchain's utility has expanded beyond financial transactions to encompass areas like blood and organ donations, as indicated by the literature survey. However, one critical aspect that has not received sufficient attention is the validation of criminal information requests for authenticity and the establishment of trust through immutability.

The validation of requests has been rigorously examined in specific contexts, such as student degree verification processes, where blockchain has demonstrated its effectiveness. Therefore, this research proposes the integration of a blockchain-based solution to validate criminal information requests. By upholding transparency, this approach allows donors to witness firsthand how their contributions are channeled towards fulfilling these requests. Blockchain technology's core principles, including transparency and the elimination of intermediaries, can be harnessed to instill trust and authenticity in the validation of criminal information requests.

The implementation of digital signatures emerges as a crucial component in this context, serving to validate the authenticity of users' requests and further fortify the trustworthiness of the criminal information management system. This is a criminal system based on the Sri Lanka police departments according to the GDPR and HIPAA. We addressed the existing problems with our proposed Blockchain technology.

4.1.Achieved research objectives.

A blockchain-based criminal information management system (BMS) is a secure, transparent, and efficient way to manage criminal information. The system eliminates the need for intermediaries, ensuring direct interactions between relevant parties within the criminal justice system. It also validates beneficiary requests for criminal information, keeps requests confidential and secure, and protects sensitive data.

The BMS enhances transparency and trustworthiness by recording all transactions and activities on a decentralized ledger. It also holds responsible parties accountable for their actions, fostering a sense of authenticity and accountability within the criminal justice system.

The BMS facilitates secure and efficient data sharing among authorized users and departments within the criminal justice system. It also seamlessly integrates with other systems used in the criminal justice ecosystem, such as court management systems, law enforcement databases, and correctional facility records.

The BMS offers a user-friendly interface with customizable dashboards and analytics tools. This empowers users to gain insights into trends, caseloads, and system performance.

The BMS ensures compliance with data privacy laws and regulations, especially concerning the handling of personally identifiable information (PII) and sensitive data. Anonymization and pseudonymization techniques are employed where applicable to protect user privacy.

Regular data backup procedures are implemented to prevent data loss in the event of system failures or emergencies. Reliable data recovery mechanisms are in place to ensure data integrity and availability.

The BMS offers several benefits for the criminal justice system, including:

- Increased efficiency and transparency

- Improved data security and privacy
- Enhanced accountability
- Seamless integration with other systems
- User-friendly interface
- Compliance with data privacy laws
- Data backup and recovery

The BMS is a promising new technology that has the potential to revolutionize the way criminal information is managed. It is a secure, transparent, and efficient way to improve the efficiency, effectiveness, and accountability of the criminal justice system.

4.2.Future Work

The prospects of blockchain technology hold immense promise on a global scale, with a significant focus on the domain of cybersecurity. While the blockchain ledger itself is public and distributed, its inherent security mechanisms ensure the safeguarding and verification of data. Employing advanced cryptography techniques, blockchain effectively mitigates vulnerabilities like unauthorized data manipulation. This robust concept of blockchain has the potential to revolutionize data management, particularly within government agencies. Its implementation can transform traditional data handling into an efficient and streamlined process, enhancing the overall performance and effectiveness of these institutions. Furthermore, blockchain's decentralized security features offer a heightened level of protection for cloud storage, significantly reducing susceptibility to hacking, data loss, or human errors when compared to centralized server-based storage.

In addition to its impact on cybersecurity, blockchain technology presents substantial opportunities within the healthcare sector. The healthcare industry in India, like many others, grapples with the challenge of insufficient data and time-consuming data compilation. Blockchain offers a solution by enabling the storage and real-time updating of crucial patient information, such as blood pressure and sugar levels, with the support of IoT devices and wearables. This transformative approach not only expedites data collection but also empowers healthcare professionals to monitor high-risk patients around the clock. In case of emergencies, blockchain facilitates instant alerts to caregivers and relatives, ensuring prompt intervention and support.

In summary, the future of blockchain technology is poised to usher in significant advancements in cybersecurity, government data management, and healthcare services. Its potential to enhance data security and streamline critical processes holds promise for a more secure and efficient digital landscape.

5. References

[1] "Coronavirus Charity Scams — What You Need to Know and How to Protect Yourself", Kaspersky.com, https://www.kaspersky.com/resource- center/threats/coronavirus-charity-scams-how-to-protect-yourself (accessed :Mar.28,2022)

[2]. "Charity and Disaster Fraud", FBI.org, https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/charity-and- disaster-fraud (accessed Apr. 15, 2022)

[3].Singh, R. Rajak, H. Mistry and P. Raut, "Aid, Charity and Donation Tracking System Using Blockchain," *2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184)*, 2020, pp. 457-462, doi: 10.1109/ICOEI48184.2020.9143001.

[4].J. Lee, A. Seo, Y. Kim, and J. Jeong, "Blockchain-Based One-Off Address System to Guarantee Transparency and Privacy for a Sustainable Donation Environment," *Sustainability*, vol. 10, no. 12, p. 4422, Nov. 2018 [Online]. Available: http://dx.doi.org/10.3390/su10124422

[5].N. Bozic, G. Pujolle and S. Secci, "A tutorial on blockchain and applications to secure network control-planes," *2016 3rd Smart Cloud Networks & Systems (SCNS)*, 2016, pp. 1-8, doi: 10.1109/SCNS.2016.7870552.

[6].Jingyu Zhang, Siqi Zhong, Tian Wang, Han-Chieh Chao, Jin Wang, "Blockchain-based Systems and Applications: A Survey," *Journal of Internet Technology*, vol. 21, no. 1 , pp. 1-14, Jan. 2020.

[7].J. Garon, "*Legal Implications of a Ubiquitous Metaverse and a Web3 Future*." https://ssrn.com/abstract=4002551),doi: http://dx.doi.org/10.2139/ssrn.4002551

[8]."Introduction to Web3" ethereum.org. https://ethereum.org/en/web3/ (accessed Jul. 25, 2022).

[9].k. Ashford, "What Is Bitcoin And How Does It Work?", forbes.com, https://www.forbes.com/advisor/investing/cryptocurrency/what-is-bitcoin (accessed June 13, 2021).

[10]. J. Abou Jaoude and R. George Saade, "Blockchain Applications – Usage in Different Domains," in *IEEE Access*, vol. 7, pp. 45360-45381, 2019, doi: 10.1109/ACCESS.2019.2902501.

[11].P. Tasatanattakool and C. Techapanupreeda, "Blockchain: Challenges and applications," *2018 International Conference on Information Networking (ICOIN),* 2018, pp. 473-475, doi: 10.1109/ICOIN.2018.8343163.“What is blockchain technology?” ibm.com. https://www.ibm.com/topics/what-is-blockchain (accessed Sept. 09, 2022).

[12]. “What is blockchain technology?” ibm.com. https://www.ibm.com/topics/what-is-blockchain (accessed Sept. 09, 2022).

[13]. D. Yaga, P. Mell, N. Roby and K. Scarfone, "Blockchain Technology Overview Draft NISTIR 8202 NIST U.S", *Journal of Cryptology*, vol. 3, no. 2, pp. 99-111, 2018.

[14]. S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” Oct. 2008. [15]. D. Newman, “Blockchain node providers and how they work,” InfoQ, 03-Mar-

2021. [Online]. Available: https://www.infoq.com/articles/blockchain-as-a-service-

get-block/. [Accessed: 06-Mar-2022].
[16]. Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain

Technology: Architecture, Consensus, and Future Trends," *2017 IEEE International Congress on Big Data (BigData Congress)*, 2017, pp. 557-564, doi: 10.1109/BigDataCongress.2017.85.

[17]. L. Wang, X. Shen, J. Li, J. Shao and Y. Yang, "Cryptographic primitives in blockchains"*,Journal of Network and Computer Application*,2019, PP.43-58, DOI:https://doi.org/10.1016/j.jnca.2018.11.003.

[18]. OAIC, "APP 2 — Anonymity and pseudonymity", Australian Government-OAIC,Sydney ,NSW 2001,2019. Accessed Jul. 22,2022. [online].Available:https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-2-app-2-anonymity-and-pseudonymity

[19]. “What is blockchain security?” ibm.com. https://www.ibm.com/topics/blockchain-security (accessed Jul. 21, 2022)

[20]. What are smart contracts on blockchain?”, ibm.com.https://www.ibm.com/topics/smart-contracts(accessed AUg. 21,2022)

[21]. “Introduction to smart contracts” ethereum.org. https://ethereum.org/en/developers/docs/smart-contracts/ (accessed Sept. 11, 2022).

[22]. JSON-RPC Working Group,"JSON-RPC 2.0 Specification", https://www.jsonrpc.org/specification (Accessed Aug. 15, 2022)

[23]“JSON-RPC API” ethereum.org. https://ethereum.org/en/developers/docs/apis/json- rpc/ (accessed Sept. 30, 2022)

[24]. M.Radaideh, N.Mohammad, M.M.Mukbil. “A proposed cloud-based platform for facilitating donation Services in support to needy-students”. *Research Square*; 2022. DOI: 10.21203/rs.3.rs-2050871/v1.

[25]. A. Singh and S. Sharma, "Implement Android Application For Book Donation," *2020 International Conference on Intelligent Engineering and Management (ICIEM)*, 2020, pp. 137-141, doi: 10.1109/ICIEM48762.2020.9160283.

[26]. “60 Years of Service – Lions Club of Colombo?” e-clubhouse.org. https://e-clubhouse.org/sites/colombo_host/ (accessed Jul. 02, 2022)

[27]. D. Hawashin *et al*., "Blockchain-Based Management of Blood Donation," in *IEEE Access*, vol. 9, pp. 163016-163032, 2021, doi: 10.1109/ACCESS.2021.3133953.

[28]. C. A. C. Yahaya, A. Firdaus, Y. Y. Khen, C. Y. Yaakub and M. F. A. Razak, "An Organ Donation Management System (ODMS) based on Blockchain Technology for Tracking and Security Purposes*,"2021 International Conference on Software Engineering & Computer Systems and 4th International Conference on Computational Science and Information Management (ICSECS-ICOCSIM)*, 2021, pp. 377-382, doi: 10.1109/ICSECS52883.2021.00075.

[29]. H. Saleh, S. Avdoshin and A. Dzhonov, "Platform for Tracking Donations of Charitable Foundations Based on Blockchain Technology," *2019 Actual Problems of Systems and Software Engineering (APSSE)*, 2019, pp. 182-187, doi: 10.1109/APSSE47353.2019.00031.

[30]. Y. Fan, C. Ao and L. Jingren, "Research on the Application Model of Public Welfare Crowdfunding Based on Blockchain Technology," *2021 2nd International Conference on E-Commerce and Internet Technology (ECIT*), 2021, pp. 441-445, doi: 10.1109/ECIT52743.2021.00098.

[31]. N.T.T.Quynh,et.al, , “Toward a Design of Blood Donation Management by Blockchain Technologies*“International Conference on Computational Science and Its Applications–ICCSA 2021*. ICCSA 2021. Lecture Notes in Computer Science(), vol 12956. Springer, Cham. https://doi.org/10.1007/978-3-030-87010-2_6

[32]. P. L. Wijayathilaka, P. H. P. Gamage, K. H. B. De Silva, A. P. P. S. Athukorala, K. A. D. C. P. Kahandawaarachchi and K. N. Pulasinghe, "*Secured, Intelligent Blood and Organ Donation Management System - “LifeShare”,"*2020 2nd International Conference on Advancements in Computing (ICAC), 2020, pp. 374-379, doi:

[33]. M.Rafi,S.Shaji,A.Thomas,”Certificate management and validation system using blockchain”, *International Research Journal of Engineering and Technology*, vol.07,no.05,pp. 7674- 7677, May.2020, Avalialble: https://www.irjet.net/archives/V7/i5/IRJET-V7I51484.pdf

[34]. C. BouSaba and E. Anderson, "Degree Validation Application Using Solidity and Ethereum Blockchain," *2019 SoutheastCon*, 2019, pp. 1-5, doi: 10.1109/SoutheastCon42311.2019.9020503.

[35]. Central Bank of Sri Lanka,"*Public Awareness in Relation to the Use of Virtual Currencies in Sri Lanka*", cbsl.gov.lk. https://www.cbsl.gov.lk/en/news/public- awareness-of-virtual-currencies-in-sri-lanka (Accessed Sept. 12, 2022)

[36]. https://ieeexplore.ieee.org/document/8584365 (accessed Jun. 19, 2021).

[37]. P. Bansal, R. Panchal, S. Bassi, and A. Kumar, “Blockchain for Cybersecurity: A Comprehensive Survey,” IEEE Xplore, Apr. 01, 2020. https://ieeexplore.ieee.org/document/9115738.

6. Appendices

Appendix A – Gantt chart for our system implementation

Group ID : **23-270**

Project Start Date : 1/1/2023

Scrolling Increment : 5

Milestone Description	Start	Days
Project Planning		
Discussion with Supervisor	1/5/2023	3
Project Component Planning	1/5/2023	15
Feasible Study of Blockchain	1/25/2023	32
Phase I		
Topic Assesment Form	3/10/2023	6
Project Charter Documenmt	3/15/2023	10
Project Proposal Documenmt	3/20/2023	4
Proposal Presentation	3/25/2023	18
SRS Document Creation	4/15/2023	13
Phase II		
Define the Requiremens & Information Gathering	5/1/2023	3
Crear a Use Case for Implementation	5/10/2023	4
Write the Requireed UI Designs	5/10/2023	80
System Development	5/15/2023	85
Progress Presentation I	5/20/2023	7
Configurations	8/1/2023	10
Phase III		
System Testing I	8/15/2023	4
System Testing II	8/20/2023	7
Phase IV		
Progress Presentation II	8/25/2023	10
Final Dissertation Report	7/30/2023	32
Phase V		
Integrate Modules	9/15/2023	6
System Testing III	9/25/2023	6
Final Report Generation	9/1/2023	35
Report Shared for Proofreading	10/10/2023	5
Presentation Creation	10/1/2023	15
Final Presentation & Viva	10/25/2023	1

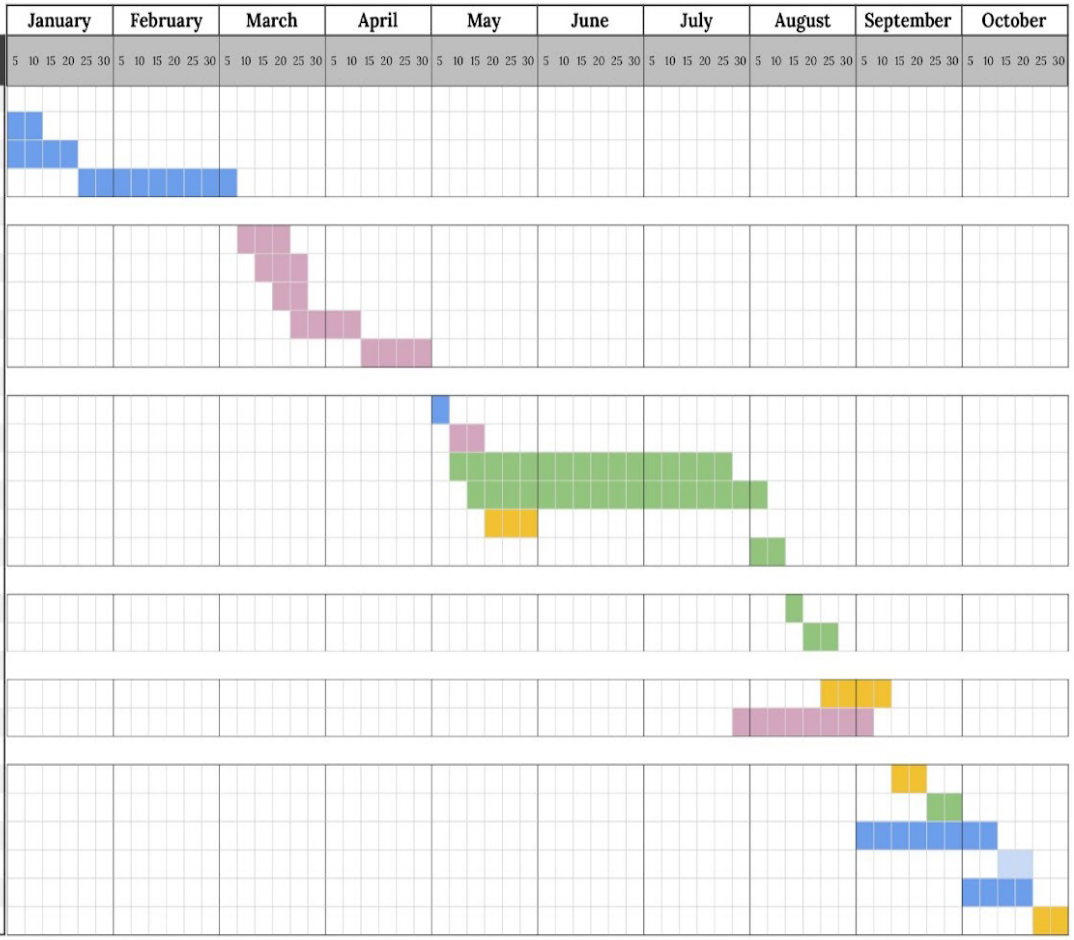


Figure 34:Gantt chart for our system implementation

Appendix B – Work breakdown structure for the Project

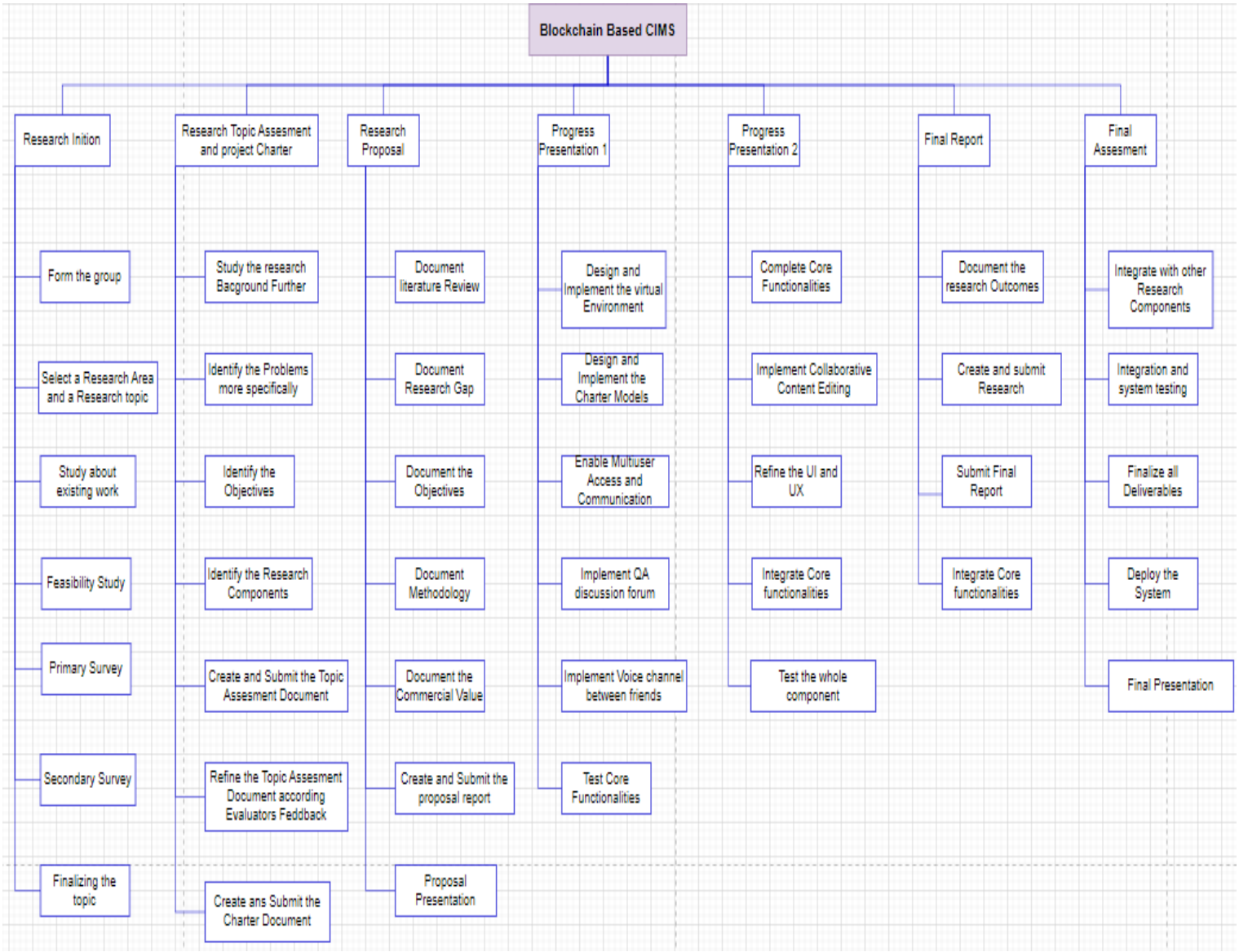


Figure 35:Work breakdown structure for the Project

Figure 36:Project main objective view