

PROJECT DOCUMENTATION

PROJECT PROPOSAL

Project: Certichain - A secure certificate verification system for Institute Santha Rita

Release: February 2024

Date: 09th February 2024

PRINCE2

Author: Nethrough Wickramasinghe (Quality Manager)

Owner: Dr. Yasas Jayaweera (Project Executive)

Client: Mr. Ravi Muditha

Version No: 1.0

PROJECT PLAN HISTORY

1.1. DOCUMENT LOCATION

This document is only valid on the day it was printed.

The source of the document will be found on the project's PC in location.

1.2. REVISION HISTORY


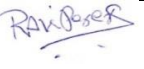
Date of this revision:

| Name | Signature | Summary of Changes | Changes marked |
|------|-----------|--------------------|----------------|
| | | | |

1.3. APPROVALS

This document requires the following approvals.

Signed approval forms are filed in the Management section of the project files.

| Name | Signature | Title | Date of Issue | Version |
|---------------------|---|-------------------|---------------|---------|
| Dr. Yasas Jayaweera | | Project Executive | 08/02/2024 | 1.0 |
| A. A. M. N Perera |  | Project Manager | 08/02/2024 | 1.0 |
| Mr. Ravi Muditha |  | Client | 08/02/2024 | 1.0 |

1.4. DISTRIBUTION

This document has been distributed to:

| Name | Title | Date of Issue | Version |
|--------------------------|--------------------|---------------|---------|
| A. A. M. N Perera | Project manager | 08/02/2024 | 1.0 |
| I. Hassaan | Start-up manager | 08/02/2024 | 1.0 |
| Nethrough Wickramasinghe | Quality manager | 08/02/2024 | 1.0 |
| Shenuka Fernando | Risk manager | 08/02/2024 | 1.0 |
| P. A Gunawardane | Scheduling manager | 08/02/2024 | 1.0 |

Table of Contents

| | |
|---|-----|
| PROJECT PLAN HISTORY | i |
| 1.1. DOCUMENT LOCATION | i |
| 1.2. REVISION HISTORY | i |
| 1.3. APPROVALS..... | i |
| 1.4. DISTRIBUTION | i |
| LIST OF TABLES | iii |
| LIST OF FIGUERS | iii |
| 1. INTRODUCTION | 1 |
| 1.1. BACKGROUND OF THE CLIENT / PROJECT | 1 |
| 1.2. PROBLEM STATEMENT..... | 1 |
| 1.3. NEEDS STATEMENT..... | 2 |
| 1.4. SOLUTION AND OBJECTIVES | 2 |
| 2. PROPOSED TECHNICAL APPROCH | 4 |
| 2.1. DEVELOPMENT METHODOLOGY | 4 |
| 2.1.1. WHY WE CHOOSE AGILE DEVELOPMENT METHODOLOGY AGILE? .. | 5 |
| 2.2. REQUIREMENT GATHERING | 5 |
| 2.3. ARCHITECTURE DIAGRAM..... | 6 |
| 2.3.1. AS IS SYSTEM..... | 6 |
| 2.3.2. TO BE SYSTEM | 7 |
| 2.4. FUNCTIONAL REQUIREMENTS | 8 |
| 2.5. NON – FUNCTIONAL REQUIREMENTS | 8 |
| 2.6. IMPLEMENTATION AND DEVELOPMENT REQUIREMENTS..... | 9 |
| 2.7. RUNNING ENVIRONMENT REQUIREMENTS | 10 |
| 2.8. QUALITY ASSURANCE PLAN..... | 10 |
| 3. EXPECTED PROJECT RESULTS | 12 |
| 3.1. DELIVERABLES..... | 13 |
| 3.2. MEASURES OF SUCCESS..... | 13 |
| 4. BUDGET | 14 |
| 5. ROLES AND RESPONSIBILITIES | 15 |
| 7. REFERENCES..... | 18 |

LIST OF TABLES

Table 1: Budget of the project.....14

Table 2: Roles and responsibilities of the project15

LIST OF FIGUERS

Figure 1: Agile Methodology.....4

Figure 2: As is System7

Figure 3: To be System.7

Figure 4: Gantt Chart16

Figure 5: Scheduled Works17

1. INTRODUCTION

Santha Rita Institute is a renowned educational institution situated in the Napoli region of Italy. This institution, with a history that spans many decades, has gained distinction as a dependable instructor. Nevertheless, the institution's authority and the legitimacy of credentials have been compromised due to the proliferation of counterfeit or unauthorized duplicates, facilitated by recent technological improvements. After recognizing this truth, the team suggested developing a web application that incorporates blockchain technology to verify and establish the authenticity of every certificate.

1.1. BACKGROUND OF THE CLIENT / PROJECT

The "Certichain" project is based on the essential need for Santha Rita Institute to enhance its certificate management system. Historically, the institution relied on a centralized system to store academic certificates, which posed significant issues such as certificate counterfeiting, unauthorized access, and system failures. These vulnerabilities not only jeopardized the security of student information but also posed a risk to the institute's reputation for excellence in education.

Acknowledging these concerns, the institution embarked on a search for a revolutionary solution that could safeguard certificate data with utmost security and reliability. The implementation of blockchain technology is a promising possibility to address these challenges. The inherent characteristics of blockchain, such as decentralization, immutability, and cryptographic security, facilitated a fundamental shift in the way certificates are handled.

1.2. PROBLEM STATEMENT

There currently exists no system for a holder of a certificate to verify its authenticity in respect to the Santha Rita institute. As this situation is one of utmost significance to the credibility of the institution it affects the ability of the organization to function. Creation of separate certificates under the pretense of the Santha Rita institute or even duplicating existing certificates under malicious intentions are the main persistent issues. Therefore, it can be

concluded that the major problem in this context is the lack of method of verification for the certification.

In order to address these risks, the project will utilize a decentralized blockchain system that ensures certificates are stored immutably and encrypted across distributed peer nodes. The cryptographic features and redundancy of the blockchain architecture remove single points of failure while safeguarding the integrity of certificates. The web application offers administrators user-friendly controls to oversee certificate management within this backend blockchain infrastructure. In conclusion, by leveraging blockchain decentralization, the project establishes an exceptionally secure and robust certificate management system for Santha Rita.

1.3. NEEDS STATEMENT

We have suggested building a website to fulfil this goal, as the requirement at hand is for the certificates' legitimacy to be verified.

1.4. SOLUTION AND OBJECTIVES

To tackle the prevailing challenges surrounding certificate security, accessibility, and administration, our proposal suggests the creation of a blockchain-powered web application system tailored to meet the specific requirements of Santha Rita. This solution consists of a user-friendly front-end application that interacts with a permissioned blockchain infrastructure designed for the storage and management of certificates on the backend.

At the heart of the system lies the blockchain, which encrypts certificates, distributes duplicates across nodes, and limits access solely to authorized personnel within the institute. Through advanced cryptographic techniques and decentralized consensus mechanisms, the integrity of certificates is safeguarded against unauthorized alterations, while the replication strategy mitigates the risk of single points of failure.

The intuitive user interface of the application serves to simplify day-to-day operations by bridging the complexities of underlying blockchain protocols. Key functionalities encompass:

- File upload capabilities supporting certificates in popular formats.
- Automated procedures for registering certificates on the blockchain.
- Search, filter, and retrieval functionalities to efficiently locate and manage existing certificates.

- Ability to view and monitor the certificate data stored on the blockchain and IPFS.
- Certificate validation.

2. PROPOSED TECHNICAL APPROCH

The "Certichain" project's technological approach uses blockchain technology to provide Santha Rita Institute a secure, decentralized certificate administration system. By utilizing blockchain, we want to solve the present problems with certificate security, integrity, and reliability. Through the implementation of redundant and immutable certificate storage among distributed nodes, this approach enhances data integrity and eliminates single points of failure. Through its user-friendly online interfaces and robust security features, CertiChain will offer Santha Rita Institute a dependable and impermeable academic credential management system.

2.1. DEVELOPMENT METHODOLOGY

The “Certichain” project will be done utilizing the Agile methodology. It is a flexible and iterative approach to software development that promotes collaboration, adaptation, and continuous improvement. Agile is well-suited for dynamic projects like CertiChain, where needs to develop over time and close engagement with client is important for success.

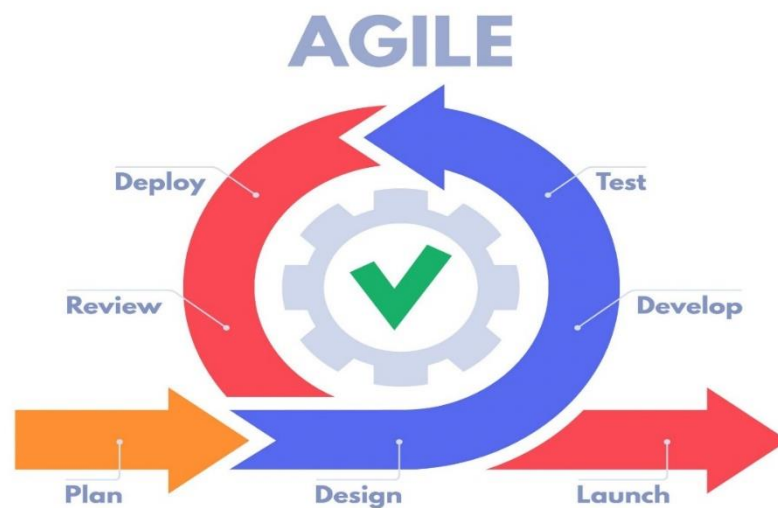


Figure 1: Agile Methodology

2.1.1. WHY WE CHOOSE AGILE DEVELOPMENT METHODOLOGY AGILE?

- **Iterative Development:** The project will be broken into short, manageable chunks called sprints. During each sprint, particular features or functions will be built, tested, and delivered.
- **Customer Engagement:** Continuous engagement with Santha Rita Institute including administrators, educators, and IT workers, we can ensure that the solution meets their requirements and expectations.
- **Adaptive Planning:** The project plan and priorities will be updated depending on information gained during client meetings and demos.
- **Continuous Integration and Testing:** Testing and continuous integration methods will be used to guarantee that new features are tested and incorporated into the current system without creating interruptions.
- **Incremental Delivery:** Working software will be released progressively at the conclusion of each sprint, enabling stakeholders to offer comments and confirm the functionality before advancing to the next iteration.

By employing an Agile methodology, the Certichain project team will be able to react rapidly to input, prioritize features based on value, and produce a high-quality solution that satisfies Santha Rita Institute's needs in a timely and efficient way.

2.2. REQUIREMENT GATHERING

Requirement collection is a critical part in the Certichain project because it creates the framework for the full development process. During this phase, the project team will interact with stakeholders from Santha Rita Institute to obtain, appraise, and record their objectives, targets, and expectations for the certificate management system. The objective is to collect complete and exact requirements that will serve as the foundation for building and executing the solution. Therefore, the tactics employed for planning and collection of information from different sources are as follows,

- Understanding of the input and output process of the current process.
- Held multiple meetings with the client to properly understand the manual procedure.
- Collecting existing resources on the project subject. Find and assess the comparable systems that might be beneficial in the development process.

2.3. ARCHITECTURE DIAGRAM

The Santha Rita Institute's current certificate management system is based on traditional centralised databases, which have built-in weaknesses include data manipulation, unauthorised access, certificate forging, and single points of failure. The current process for managing academic credentials is laborious, error-prone, and unable to keep up with the institute's increasing requirements. Nonetheless, Santha Rita Institute hopes to change its certificate administration procedure with the implementation of the CertiChain initiative.

The institution will transition from a manual, paper-based approach to a secure, decentralised, and user-friendly certificate management platform by integrating blockchain technology and contemporary web application development standards. Features like staff dashboards, authorization limitations, search and retrieval capabilities, and redundant storage across encrypted blockchain nodes are all part of this new system. Santha Rita Institute will improve data security and integrity, streamline administrative, instructional, and student experiences, and streamline certificate administration processes with CertiChain.

2.3.1. AS IS SYSTEM

Currently, the Santha Rita Institute manually enters all the Certificate information to a centralized database and hand over a printed copy to the students. They don't have a way to authenticate the certificates.

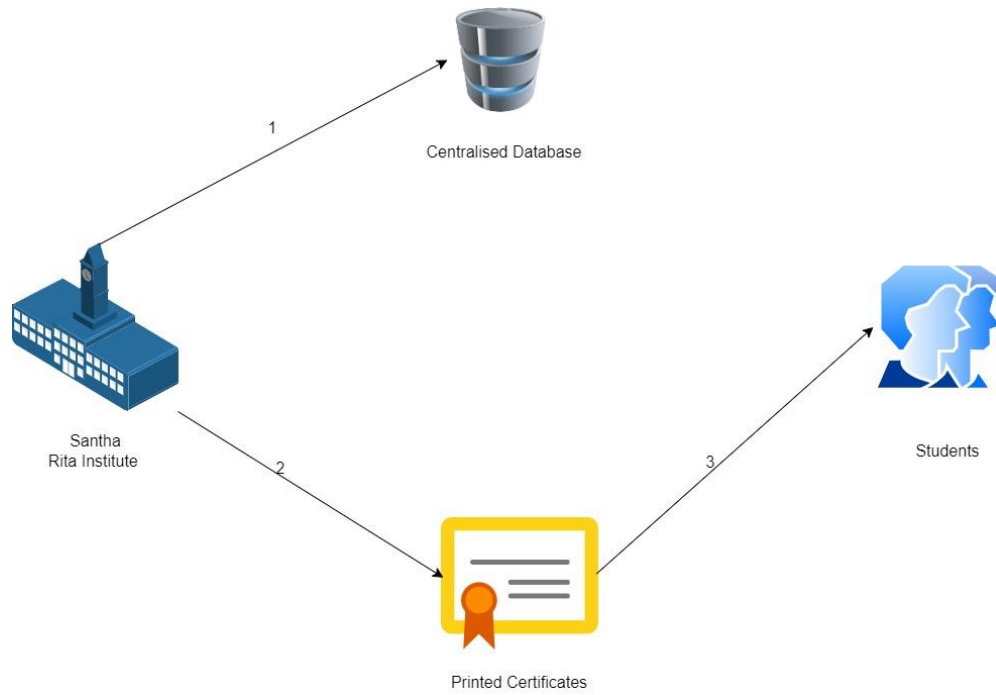


Figure 2: As is System

2.3.2. TO BE SYSTEM

The system's functionality is divided into services, each of which is offered by a system application.

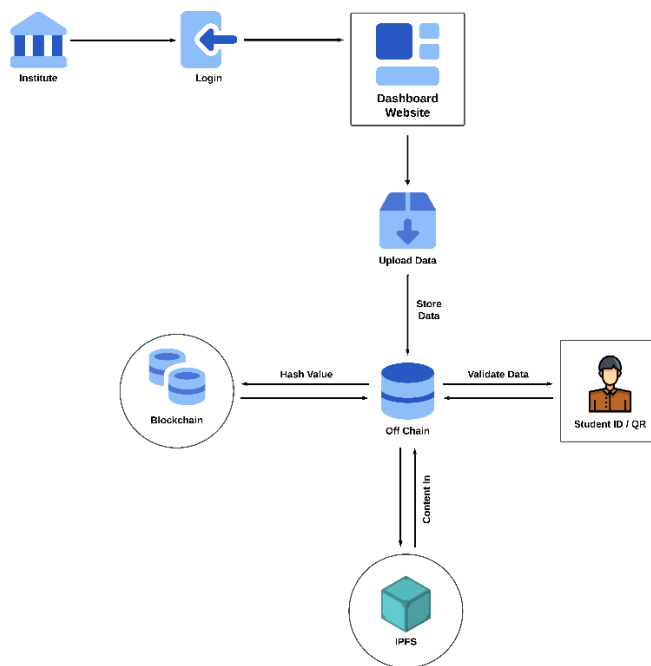


Figure 3: To be System.

2.4. FUNCTIONAL REQUIREMENTS

1. **User Authentication** - The system will support different permission levels for institute staff. Admin users can manage other users and certificates while standard users have read access.
2. **Certificate Uploads** - Authorized staff users can upload academic certificates via the web application.
3. **Blockchain Integration** - The system will interface with a permissioned blockchain to securely store certificate records in a redundant and encrypted manner across decentralized nodes.
4. **Search and Retrieval** - The application will allow staff users to conveniently search and retrieve certificates.
5. **Certificate Verification** - The blockchain integration will enable verification of authenticity and integrity for retrieved certificates through hashing and digital signatures.

2.5. NON – FUNCTIONAL REQUIREMENTS

1. Security:
 - The system will employ encryption using industry standard algorithms to protect sensitive certificate data in transit and at rest.
 - External security audits will be conducted to identify and resolve application vulnerabilities through testing.
2. Availability:
 - Decentralized blockchain infrastructure will ensure high availability of certificate records without single points of failure.
 - Redundancy features like load balancing, failover and automatic recovery will enable 24/7 access with minimal downtime.
3. Usability:
 - The web interface will offer simple, intuitive navigation and workflows optimized for certificate management tasks by institute staff.
 - Contextual help, user guides and on-screen interactive tips will assist staff users adapt to the new system.
4. Performance:
 - Blockchain network selection, node configuration and caching mechanisms will optimize response times for certificate transactions.

- Load testing will gauge peak capacity limits for concurrent user access to cater to usage surges like during enrolments.

2.6. IMPLEMENTATION AND DEVELOPMENT REQUIREMENTS

Software requirements

- MySQL Server
- Visual Studio Code
- Libraries- Bootstrap
- Microsoft word
- Microsoft PowerPoint
- Windows 7 / MAC OS X or above
- IPFS
- Chelo Blockchain

Hardware requirements

- PC
- WIFI router
- CPU i3 or above
- RAM - 4GB or above
- Disk - 20GB.

2.7. RUNNING ENVIRONMENT REQUIREMENTS

Recommended requirements:

- Windows 10 / Mac OS X Desktop
- 2 GHz or above processor
- 32 / 64 – bit processor
- Disk - 20GB.
- Web browser.

2.8. QUALITY ASSURANCE PLAN

This quality assurance (QA) plan outlines the strategy and procedures for testing and validating the blockchain-based certificate management web application for Santha Rita Institute. By executing a rigorous QA process, we aim to verify all intended functionality, usability, security, and performance requirements before deployment.

1. Objectives:

- Validate correct working of key certificate management workflows.
- Evaluate interface usability and user experience.
- Verify security standards compliance.
- Ensure optimal response times/scalability.

2. Test Strategy:

- Functionality testing - Validate certificate transactions, retrieval, verification against specs.
- UI/UX testing – User workflow and acceptance testing
- Performance testing – Stress testing and bottleneck identification
- Security audits – Static analysis, vulnerability scanning, penetration testing

3. Test Scope:

- Certificate upload, storage, search, sharing.
- Administrative interfaces and controls
- Blockchain integration and API layers
- Access controls and encryption
- Notifications, monitoring, and logging

4. Test Plans:

- Functional & integration test plans
- UAT test plans
- Performance benchmark requirements
- Security standards compliance checklist

3. EXPECTED PROJECT RESULTS

The primary goal of implementing the secure certificate verification system at Santha Rita Institute is to enhance the security, reliability, and efficiency of academic certificate management through blockchain technology. This initiative aims to transition from a traditional, manual, and centralized system of certificate storage to a decentralized, digital blockchain-based system.

The expected project results encompass several key areas:

- **Development of a Robust Web Application:** The project will culminate in the creation of a secure, user-friendly web application. This platform will serve as the primary interface for certificate management, allowing authorized staff to upload, store, retrieve, and verify academic certificates with ease.
- **Blockchain Integration for Enhanced Security:** By leveraging blockchain technology, the system will ensure the immutability and encryption of certificate data, significantly reducing the risks associated with hacking, data tampering, and duplication.
- **Efficient Certificate Management Capabilities:** The system will streamline the management of certificates. Features will include certificate issuance, secure storage, easy retrieval for verification purposes, and real-time updates of certificate status.
- **Administrative Efficiency and User Accessibility:** The project will provide a tailored administrative module for Santha Rita Institute's staff, equipped with features such as a comprehensive dashboard for monitoring and managing certificates.
- **Verify Certificates:** The system will allow the students to include the certificate ID to check whether the certificate is verified or not.
- **Compliance with High Security and Privacy Standards:** The system will adhere to the latest cybersecurity protocols and privacy regulations, ensuring the protection of sensitive academic information.
- **Scalability and Futureproofing:** The system will be designed with scalability in mind, allowing for future enhancements and the integration of additional functionalities as needed.

3.1. DELIVERABLES

- Project brief
- Project proposal
- Software requirement specification report
- Prototypes
- Progress review
- Final product

3.2. MEASURES OF SUCCESS

- **User Adoption Rate:** The percentage of institute staff actively using the system for certificate management tasks.
- **System Reliability:** Measured by the uptime of the web application and the successful execution of certificate management processes without errors or system downtimes.
- **Data Integrity and Security:** The successful storage and retrieval of certificates with no data corruption or security breaches. This can be quantified by the absence of security incidents or data integrity issues.
- **Staff Satisfaction:** Assessed through surveys and feedback from the institute's staff regarding ease of use, efficiency, and overall satisfaction with the system.
- **Response and Processing Time:** The time taken by the system to upload, retrieve, and verify certificates, aiming for minimal latency in these operations.
- **Regulatory Compliance:** Adherence to relevant data protection and privacy regulations, as evidenced by compliance audits and assessments.

4. BUDGET

| Expenses | Description | Basis | Unit | Rate | Total |
|------------------------------------|---|---------------|------|--------|---------------|
| Planning | | | | | |
| Meetings (Zoom Meetings) | Internet charges | Hourly | 10 | 200 | 2 000 |
| Development | | | | | |
| Designing UIs | Design UIs for the website | Per hour | 12 | 1000 | 12 000 |
| Website implementation | Implement functions according to the designed UIs | Hourly | 45 | 800 | 36 000 |
| Blockchain Gateway | Harmony Blockchain | Per data | 100 | 30 | 3 000 |
| FileBase | IPFS File Storage | Per data | 100 | 100 | 10 000 |
| Database design and implementation | Develop a database and store data | Hourly | 12 | 700 | 8 400 |
| Testing | | | | | |
| QA testing | Check the quality of the site | Hourly | 5 | 500 | 2 500 |
| Documentation | | | | | |
| Preparation of documentation | Prepare required documents for the project | All documents | N/A | N/A | 4 000 |
| Setting up | | | | | |
| Domain | Domain name for the website | Per year | 1 | 3600 | 3 600 |
| Hosting | Hosting the website and the database | Per year | 1 | 15 000 | 15 000 |
| Total | | | | | 96 500 LKR |

Table 1: Budget of the project

5. ROLES AND RESPONSIBILITIES

| Role | Name | Responsibility |
|--------------------|--------------------------|---|
| Project Sponsor | Mr. Ravi Muditha | Sponsoring the project |
| Project Manager | A. A. M. N. Perera | <ul style="list-style-type: none"> Requirement Gathering. Analyzing. Communicating with the Client. Directing the team and updating them. Managing the team, resources, schedules, and deliverables |
| Start-up manager | I. Hassaan | <ul style="list-style-type: none"> Ensuring the website's effective launch and initial operations. Strategic planning, acquiring resources, adhering to the law, establishing a team, managing finances, supervising operations, marketing, and performance evaluation. |
| Quality manager | Nethrough Wickramasingha | <ul style="list-style-type: none"> Quality assurance of the final product. Setting quality goals, performing tests and inspections. Fostering continuous improvement, |
| Risk manager | Shenuka Fernando | <ul style="list-style-type: none"> Locating, evaluating, and reducing risks. Identify potential risks, assessing their possibility and impact, creating mitigation measures, keeping an eye on risk indicators. |
| Scheduling manager | Pasindu Gunawardane | <ul style="list-style-type: none"> Developing and overseeing the project timeline. Planning project timetables, keeping track of progress, modifying schedules as necessary, working with team members, and communicating routine schedule updates to stakeholders |

Table 2: Roles and responsibilities of the project

6. SCHEDULE

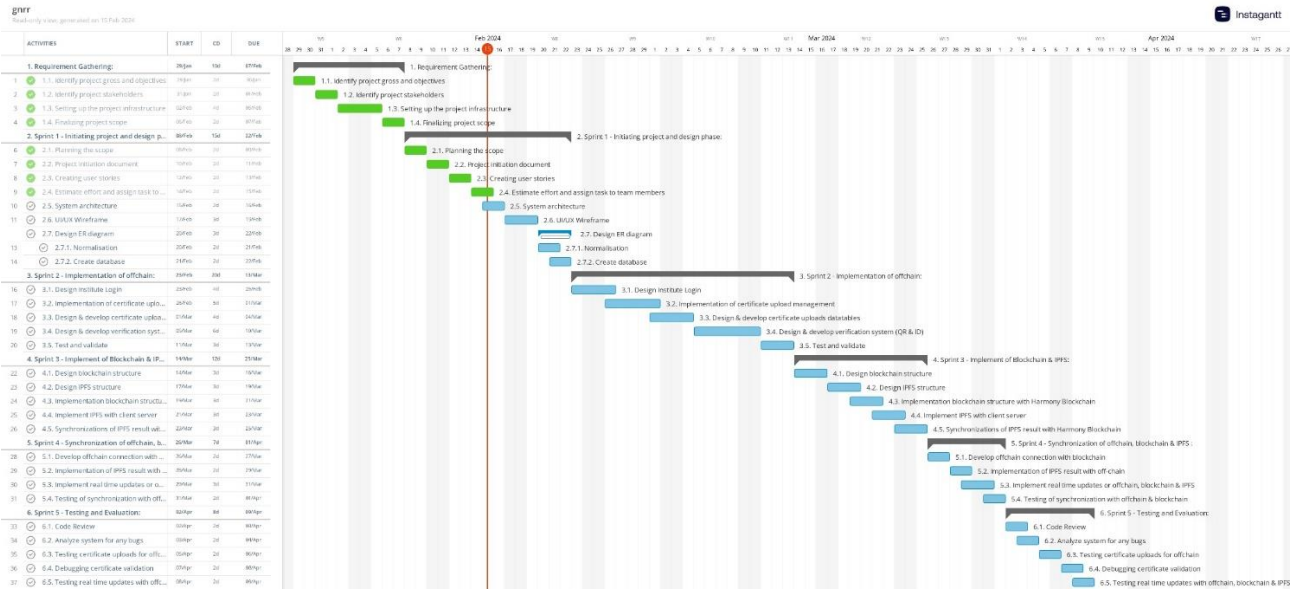


Figure 4: Gantt Chart

| | ACTIVITIES | START | CD | DUE |
|----|--|---------------|------------|---------------|
| | 1. Requirement Gathering: | 29/Jan | 10d | 07/Feb |
| 1 | ✓ 1.1. Identify project gross and objectives | 29/Jan | 2d | 30/Jan |
| 2 | ✓ 1.2. Identify project stakeholders | 31/Jan | 2d | 01/Feb |
| 3 | ✓ 1.3. Setting up the project infrastructure | 02/Feb | 4d | 05/Feb |
| 4 | ✓ 1.4. Finalizing project scope | 05/Feb | 2d | 07/Feb |
| | 2. Sprint 1 - Initiating project and design p... | 08/Feb | 15d | 22/Feb |
| 6 | ✓ 2.1. Planning the scope | 08/Feb | 2d | 09/Feb |
| 7 | ✓ 2.2. Project initiation document | 10/Feb | 2d | 11/Feb |
| 8 | ✓ 2.3. Creating user stories | 12/Feb | 2d | 13/Feb |
| 9 | ✓ 2.4. Estimate effort and assign task to ... | 14/Feb | 2d | 15/Feb |
| 10 | ⊙ 2.5. System architecture | 15/Feb | 2d | 16/Feb |
| 11 | ⊙ 2.6. UI/UX Wireframe | 17/Feb | 3d | 19/Feb |
| | ⊙ 2.7. Design ER diagram | 20/Feb | 3d | 22/Feb |
| 13 | ⊙ 2.7.1. Normalisation | 20/Feb | 2d | 21/Feb |
| 14 | ⊙ 2.7.2. Create database | 21/Feb | 2d | 22/Feb |
| | 3. Sprint 2 - Implementation of offchain: | 23/Feb | 20d | 13/Mar |
| 16 | ⊙ 3.1. Design Institute Login | 23/Feb | 4d | 26/Feb |
| 17 | ⊙ 3.2. Implementation of certificate uplo... | 26/Feb | 5d | 01/Mar |
| 18 | ⊙ 3.3. Design & develop certificate uploa... | 01/Mar | 4d | 04/Mar |
| 19 | ⊙ 3.4. Design & develop verification syst... | 05/Mar | 6d | 10/Mar |
| 20 | ⊙ 3.5. Test and validate | 11/Mar | 3d | 13/Mar |
| | 4. Sprint 3 - Implement of Blockchain & IP... | 14/Mar | 12d | 25/Mar |
| 22 | ⊙ 4.1. Design blockchain structure | 14/Mar | 3d | 16/Mar |
| 23 | ⊙ 4.2. Design IPFS structure | 17/Mar | 3d | 19/Mar |
| 24 | ⊙ 4.3. Implementation blockchain structu... | 19/Mar | 3d | 21/Mar |
| 25 | ⊙ 4.4. Implement IPFS with client server | 21/Mar | 3d | 23/Mar |
| 26 | ⊙ 4.5. Synchronizations of IPFS result wit... | 23/Mar | 3d | 25/Mar |
| | 5. Sprint 4 - Synchronization of offchain, b... | 26/Mar | 7d | 01/Apr |
| 28 | ⊙ 5.1. Develop offchain connection with ... | 26/Mar | 2d | 27/Mar |
| 29 | ⊙ 5.2. Implementation of IPFS result with ... | 28/Mar | 2d | 29/Mar |
| 30 | ⊙ 5.3. Implement real time updates or o... | 29/Mar | 3d | 31/Mar |
| 31 | ⊙ 5.4. Testing of synchronization with off... | 31/Mar | 2d | 01/Apr |
| | 6. Sprint 5 - Testing and Evaluation: | 02/Apr | 8d | 09/Apr |
| 33 | ⊙ 6.1. Code Review | 02/Apr | 2d | 03/Apr |
| 34 | ⊙ 6.2. Analyze system for any bugs | 03/Apr | 2d | 04/Apr |
| 35 | ⊙ 6.3. Testing certificate uploads for offc... | 05/Apr | 2d | 06/Apr |
| 36 | ⊙ 6.4. Debugging certificate validation | 07/Apr | 2d | 08/Apr |
| 37 | ⊙ 6.5. Testing real time updates with offc... | 08/Apr | 2d | 09/Apr |

Figure 5: Scheduled Works

7. REFERENCES