

Interim Report
Level 2
Blockchain Based Vehicle Registration and Ownership Management
System
Troyrangers

| | |
|----------------------|---------|
| Dissanayake D.M.B.M. | 204047J |
| Herath P.A.U.D. | 204074M |
| Jayathilaka P.H.P. | 204087F |
| Pathirana S.P.S.N. | 204150T |
| Rathnayaka A.M.D.B. | 204179N |

Faculty of Information Technology
University of Moratuwa
2022

Interim Report
Level 2
Blockchain Based Vehicle Registration and Ownership Management
System
Troyrangers

| | |
|----------------------|---------|
| Dissanayake D.M.B.M. | 204047J |
| Herath P.A.U.D. | 204074M |
| Jayathilaka P.H.P. | 204087F |
| Pathirana S.P.S.N. | 204150T |
| Rathnayaka A.M.D.B. | 204179N |

Supervised by:
Dr. Thanuja A.L.A.R.R.
Department of Computational Mathematics
University of Moratuwa

.....
(Signature)

Faculty of Information Technology
University of Moratuwa
2022

Abstract

In the modern day and age, the security of data has a higher priority. Especially the ownership of a vehicle must not be changed by others unnecessarily. But when using a centralized database unauthorized people can change data and we can't track those changes. Therefore, this is a huge security burden for this kind of high-transparency system. Therefore, "Crede Technologies" company wants to provide a solution to this problem.

Considering their requirements, we decided to design the Vehicle Registration and Ownership Management System which is an application that facilitates digitizing the system of registering and transferring vehicle ownership with the use of Blockchain technology and non-fungible tokens are used for representing the vehicles. Users who want to sell or buy vehicles in a secure manner can use this application.

To provide a better application we analyze our customer requirements and design the unified model language diagrams before implementation. For developing our system, we chose technologies after a better research program. ReactJS, NextJS, and React Native for the frontend and Django for backend of our system.

In conclusion, our project has demonstrated the feasibility of using blockchain technology to create a secure and efficient vehicle registration and ownership management system. Our system has the ability to track vehicle ownership and transfer, as well as store and verify important documents such as titles and registration certificates. These capabilities have the potential to streamline the process of buying and selling vehicles and reduce the risk of fraud or errors in the vehicle ownership process. Further development and testing of the system is needed to fully realize its potential, but our results show promise for the use of blockchain technology in this application.

Table of Content

| | | |
|-----------|-----------------------------------------------------------------------------------------------------------------------------|----|
| Chapter 1 | Introduction..... | 1 |
| 1.1 | Introduction | 1 |
| 1.2 | Background Motivation..... | 2 |
| 1.3 | Major Issue – Mutability | 3 |
| 1.4 | Aim and Objectives | 3 |
| 1.5 | Summary | 4 |
| Chapter 2 | Blockchain-Based Vehicle Registration and Ownership Management Literature Review..... | 5 |
| 2.1 | Introduction | 5 |
| 2.2 | Vehicle Registration and Information Management using Blockchain-Based Distributed Ledger from Bangladesh Perspective | 5 |
| 2.3 | Sandbox | 6 |
| 2.4 | OpenSea | 7 |
| 2.5 | Summary | 8 |
| Chapter 3 | Adapted Technologies | 9 |
| 3.1 | Introduction | 9 |
| 3.2 | Web2 | 9 |
| 3.2.1 | ReactJS..... | 9 |
| 3.2.2 | React Native..... | 10 |
| 3.2.3 | NextJS | 11 |
| 3.2.4 | Django..... | 12 |
| 3.2.5 | PostgreSQL..... | 12 |
| 3.3 | Web3 | 12 |
| 3.3.1 | Blockchain | 13 |
| 3.3.2 | Aries Cloud Agent - Python..... | 15 |
| 3.3.3 | MetaMask Wallet..... | 16 |
| 3.4 | Docker | 17 |
| 3.4.1 | Docker Compose..... | 17 |
| 3.5 | Summary | 18 |
| Chapter 4 | Our Approach..... | 19 |
| 4.1 | Introduction | 19 |
| 4.2 | Blockchain-Based Vehicle Registration and Ownership Management System | 19 |
| 4.3 | Users, Inputs, Outputs of the System | 20 |
| 4.4 | Systems Working Behavior..... | 21 |
| 4.5 | Software Process Model..... | 23 |
| 4.6 | Summary | 23 |

| | | |
|------------|-----------------------------------------------------|----|
| Chapter 5 | Analysis and Design | 24 |
| 5.1 | Introduction | 24 |
| 5.2 | Analysis..... | 24 |
| 5.3 | Design..... | 24 |
| 5.3.1 | Use case Diagram | 24 |
| 5.3.2 | Activity Diagram | 25 |
| 5.3.3 | Class Diagram..... | 32 |
| 5.3.4 | Sequence Diagram | 32 |
| 5.3.5 | ER Diagram | 39 |
| 5.4 | Summary | 39 |
| Chapter 6 | Implementation | 40 |
| 6.1 | Introduction | 40 |
| 6.2 | SSI Issuer..... | 40 |
| 6.3 | SSI Verifier | 40 |
| 6.4 | Mobile SSI Wallet..... | 40 |
| 6.5 | NFT Minter | 41 |
| 6.6 | NFT marketplace..... | 41 |
| 6.7 | Triggers and Implementation | 41 |
| 6.8 | Version Controlling..... | 41 |
| 6.9 | Summary | 42 |
| Chapter 7 | Discussion..... | 43 |
| 7.1 | Introduction | 43 |
| 7.2 | Evaluation and Testing..... | 43 |
| 7.3 | How Our Solution Differs from Other Solutions | 43 |
| 7.4 | Further Development..... | 44 |
| 7.5 | Summary | 44 |
| Chapter 8 | References..... | 45 |
| Appendix A | - Individual Contribution..... | 48 |
| Appendix B | | 53 |
| Appendix C | – Plan of Action..... | 58 |
| Appendix D | – User Stories | 59 |
| Appendix E | – SRS | 60 |

List of Figures

| | |
|--------------------------------------------------------------------------------|----|
| Figure 3-1 Overview of the Architecture of the Aries Cloud Agent - Python..... | 16 |
| Figure 4-1 User, Input, Output Diagram..... | 21 |
| Figure 5-1 Use case Diagram..... | 25 |
| Figure 5-2 Activity Diagram of Issuing SSI process | 26 |
| Figure 5-3 Activity Diagram Verifying SSI Process | 27 |
| Figure 5-4 Activity Diagram saving newly created SSI | 28 |
| Figure 5-5 Minting NFT for Vehicle | 29 |
| Figure 5-6 Activity Diagram NFT Market Place to sell vehicle..... | 30 |
| Figure 5-7 Activity Diagram NFT Market Place to buy vehicle | 31 |
| Figure 5-8 Class Diagram | 32 |
| Figure 5-9 Sequence Diagram SSI Issuer | 33 |
| Figure 5-10 Sequence Diagram SSI Verifier (Web UI)..... | 34 |
| Figure 5-11 Sequence Diagram SSI Verifier (via API) | 35 |
| Figure 5-12 Sequence Diagram Mobile SSI Wallet | 36 |
| Figure 5-13 Sequence Diagram NFT Minter | 37 |
| Figure 5-14 Sequence Diagram NFT Market Place (Login with SSI)..... | 37 |
| Figure 5-15 Sequence Diagram NFT Market Place (to buy a vehicle)..... | 38 |
| Figure 5-16 Sequence Diagram NFT Market Place (to sell a vehicle) | 38 |
| Figure 5-17 ER Diagram..... | 39 |
| Figure 6-1 Version Controlling GitHub platform..... | 41 |
| Figure 8-1 Mockup Mobile SSI Wallet | 53 |
| Figure 8-2 Example of Generated QR code..... | 53 |
| Figure 8-3 Mockup of SSI Issuing Application..... | 54 |
| Figure 8-4 Mockup of UI NFT Minting Application..... | 54 |
| Figure 8-5 Implementation Backend 204047J | 55 |
| Figure 8-6 Implementation Backend 204087F | 55 |
| Figure 8-7 Implementation Backend 204150T | 56 |
| Figure 8-8 Implementation Backend 204179N..... | 56 |
| Figure 8-9 Jira as Project Management tool | 57 |

List of Abbreviations

| Abbreviation | Meaning |
|--------------|------------------------------------------------------|
| DeFi | Decentralized Financing |
| EIP | Ethereum Improvement Proposals |
| ERC | Ethereum Request for Comment |
| ETH | Ethereum |
| IPFS | Inter Planetary File System |
| NFT | Non-Fungible Token |
| RTA | Road Transport Authority |
| MVT | Model View Template |
| DLT | Distributed Ledger Technology |
| ACA-Py | Aries Cloud Agent Python |
| VOMS | Vehicle Registration and Ownership Management System |
| SRS | Software Requirement Specification |
| QR | Quick Response |
| HTTP | Hypertext Transfer Protocol |
| POC | Proof of Concept |

Chapter 1 Introduction

1.1 Introduction

Due to the development of blockchain, centralized organizations can be replaced with a decentralized collection of assets and participants. In 2014, Ethereum, a second-generation blockchain was released and it enabled programmers to execute smart contracts on a distributed ledger. Developers and companies can design financial apps using smart contracts that leverage cryptocurrencies and other token types of things like decentralized financing (DeFi), crowdfunding, decentralized exchanges, data archiving, etc. Recent developments in distributed ledger technology have produced ideas that simplify value exchange.

Today, digital assets might be represented as tokens that existed in the blockchain network by utilizing the benefits of blockchain and considering the governance concerns, which simplifies their transmission and traceability, boosts their transparency, and strengthens their security. In the context of blockchain technology, there are two main categories of tokens: fungible tokens, where each token has an identical value, and non-fungible tokens (NFTs), which have special properties and cannot be exchanged. Non-fungible tokens are digital assets with a special ID that are kept on a blockchain. The concept of NFT was first introduced in Ethereum Improvement Proposals (EIP)-721 and then developed in EIP-1155. Beginning in early 2021, NFTs developed into one of the most popular blockchain applications that attracted attention on a global scale. They might be computer recreations of actual things.

The ownership of digital goods (such as images, music, movies, and virtual creations) that can be traded is documented in blockchain smart contracts. As one of the first NFTs on Ethereum, CryptoPunks has created approximately 10,000 collectible punks and contributed to the growth of the ERC - 721 Standard [1]. In our Blockchain Based Vehicle Registration and Ownership Management System, we are minting an NFT for the purpose of representing a vehicle as a digital asset.

1.2 Background Motivation

Digitizing nonreal things has been tested until now. But digitizing real-world things has not yet. Our project is mainly focusing on changing the ownership of a vehicle online. That means this system will be used to digitize a real-world thing like a vehicle. This ownership transfer of vehicles can't be done transparently and securely using a centralized database. A centralized database is essentially a database type that is kept, located, and maintained exclusively in a single place [2]. But to address this problem using blockchain technology gives more additional features. Blockchain is a decentralized, immutable database that makes it easier to track assets and record transactions in a corporate network [3].

A centralized database and a blockchain have differences according to their architecture, immutability, data handling, and transparency. Due to the immutability, transparency, and security of these blockchains, it is better to use blockchain technology to address our problem. Because transferring vehicle ownership has to be more secure [4]. If anyone needs to change data in a blockchain that hacker has to change more than fifty percent of that blockchain nodes, and it is impractical to do such a thing. That's why blockchains come in handy for secure transactions like changing vehicle ownership. Nowadays, NFT (Non-Fungible Tokens) is very popular among investors due to the digital value given to intangible things. One of the major reasons which resulted in this popularity is the blockchain technology that is used behind these systems. NFTs, or non-fungible tokens, are blockchain-based tokens that individually represent a special asset like a work of art, a piece of digital material, or other media [5]. Nowadays although all the systems are computerized in many fields there can happen, changing data without permission. It is a huge problem today.

A centralized database and a blockchain have differences according to their architecture, immutability, data handling, and transparency. Due to the immutability, transparency, and security of these blockchains, it is better to use blockchain technology to address our problem. Because transferring vehicle ownership has to be more secure [4]. If anyone needs to change data in a blockchain that hacker has to change more than fifty percent of that blockchain nodes, and it is impractical to do such a thing. That's why blockchains come in handy for secure transactions like changing vehicle ownership. Nowadays, NFT (Non-Fungible Tokens) is very popular among investors

due to the digital value given to intangible things. One of the major reasons which resulted in this popularity is the blockchain technology that is used behind these systems. NFTs, or non-fungible tokens, are blockchain-based tokens that individually represent a special asset like a work of art, a piece of digital material, or other media [5]. Nowadays although all the systems are computerized in many fields there can happen, changing data without permission. It is a huge problem today.

Therefore, our reference company “Crede Technologies” have come up with a great idea to allow digital information to be recorded and distributed, but not edited. They wanted to do this process related to the vehicle ownership field. Therefore, we decided to use Blockchain Technology to develop their intention as our project. Nowadays in Sri Lanka, still the vehicle registering and transferring process is done through physical documents and computerized somewhat far. But it will be a great investment if we can introduce this system to Sri Lanka.

1.3 Major Issue – Mutability

The word "mutability" refers to the attribute of changeability [6]. Ownership of a vehicle must not be changed by others unnecessarily. But when using a centralized database unauthorized people can change data and we can't track those changes. Therefore, this is a huge security burden for this kind of high transparency needed system. This is our major problem.

The word "mutability" refers to the attribute of changeability [6]. Ownership of a vehicle must not be changed by others unnecessarily. But when using a centralized database unauthorized people can change data and we can't track those changes. Therefore, this is a huge security burden for this kind of high transparency needed system. This is our major problem.

1.4 Aim and Objectives

Aim: The aim of our project is to develop a system for registering and transferring vehicle ownership from one person to another in a secure manner with the use of Blockchain Technology.

Objectives:

- Study the problem of registering and transferring vehicle ownership from one person to another through documentation.

- Facilitate digitizing the system of registering and transferring vehicle ownership from one person to another.
- Create the ability to generate a digital id for verifying person and vehicle identity.
- Design the appropriate system including all user requirements.
- Develop the system for solving the problem.
- Evaluation of the proposed solution.
- Preparation of final documentation.

1.5 Summary

Through Chapter one of this report, we provide a basic introduction to the vehicle registration and ownership management system that we expect to develop. In the next chapter, similar projects for this project will be mentioned and discussed the differences between those projects and ours.

Chapter 2 Blockchain-Based Vehicle Registration and Ownership Management Literature Review

2.1 Introduction

In the previous chapter, we took an introduction about our project and what is the reason to build this project and what our aim and objectives related to this project. This chapter mainly focuses on the projects, and applications which are solutions to our problem. Though these solutions may offer some respite from the problem at hand, they ultimately fall short of fully resolving the issue at hand. Even though all these existing projects mainly focus on creating NFTs, they are not creating NFTs for physical assets. Let's go through the real-world applications which were already implemented.

2.2 Vehicle Registration and Information Management using Blockchain-Based Distributed Ledger from Bangladesh Perspective

In Bangladesh, motor vehicles should be registered in order to establish and preserve a record of the corresponding owner, and they are controlled access by the Road Transport Authority (RTA). Typically, there are several RTA locations located around the country, and the government offers services for vehicle registration by having the owner complete a standard form with the necessary identification details. The data is utilized for changing ownership, authenticating vehicles, and verifying ownership.

In contrast, as part of the existing motor vehicle registration procedure, the Bangladesh Road Transport Authority (BRTA) keeps all the data associated with a motor vehicle's registration in one main database. Due to the serious security flaws in centralized systems and the increasing number of cyberattacks globally, a hacked system's single point of failure could result in a catastrophic loss. In addition, the registration process is laborious and requires manual record input, which encourages dishonest intermediaries (like brokers) to get involved. Distributed ledgers built on the blockchain have improved the security, decentralization, and transparency of the data.

In recent years, Blockchain has been widely employed for the deployment of numerous technical systems to enforce and improve through decentralization. As a result, they suggest a Blockchain-based vehicle registration and information management system that streamlines the registration procedure and keeps transparent records of ownership

data. A few problems with the present or traditional paper-based approach to motor vehicle registration, including processing delays, drawn-out verification procedures, and a lack of obvious transparency, are addressed by the planned Blockchain system[7]. This is only a concept, and this project had not been implemented. And also, NFTs are not used in this project. However, it is our intent to take this project beyond mere theory and into the realm of practical implementation. In recent years, Blockchain has been widely employed for the deployment of numerous technical systems to enforce and improve through decentralization. As a result, they suggest a Blockchain-based vehicle registration and information management system that streamlines the registration procedure and keeps transparent records of ownership data. A few problems with the present or traditional paper-based approach to motor vehicle registration, including processing delays, drawn-out verification procedures, and a lack of obvious transparency, are addressed by the planned Blockchain system[7]. This is only a concept, and this project had not been implemented. And also, NFTs are not used in this project. However, it is our intent to take this project beyond mere theory and into the realm of practical implementation.

2.3 Sandbox

Decentraland is one of a new generation of virtual worlds, popularly referred to as metaverses, built on the blockchain. To become a citizen, all users need is to buy LAND, a coded piece of the metaverse that translates to a 16m-by-16m plot of virtual land[8]. The assets in the metaverses are NFTs, which are digital assets on blockchains that can be used to indicate ownership of identifiable things like artwork, collectibles, and other artifacts. Blockchains enable the metaverses to have their own cryptocurrencies and, as a result, their own financial ecosystems, offering a fresh environment to test monetary ideas.

Decentraland is one of a new generation of virtual worlds, popularly referred to as metaverses, built on the blockchain. To become a citizen, all users need is to buy LAND, a coded piece of the metaverse that translates to a 16m-by-16m plot of virtual land[8]. The assets in the metaverses are NFTs, which are digital assets on blockchains that can be used to indicate ownership of identifiable things like artwork, collectibles, and other artifacts. Blockchains enable the metaverses to have their own

cryptocurrencies and, as a result, their own financial ecosystems, offering a fresh environment to test monetary ideas.

The Sandbox was first released in 2012 for iOS and Android as a game. It was rebuilt on the Ethereum blockchain in 2018. Users are able to buy LAND and build ASSET to be used in the ecosystem, creating it one of the most well-known metaverses. LANDs are NFTs that represent distinctive digital real estate (identified by coordinates), and 166,464 LANDs (408 x 408) make up the map of The Sandbox metaverse. It is possible to buy and sell each LAND either individually or as part of an estate[9].

The Sandbox was first released in 2012 for iOS and Android as a game. It was rebuilt on the Ethereum blockchain in 2018. Users are able to buy LAND and build ASSET to be used in the ecosystem, creating it one of the most well-known metaverses. LANDs are NFTs that represent distinctive digital real estate (identified by coordinates), and 166,464 LANDs (408 x 408) make up the map of The Sandbox metaverse. It is possible to buy and sell each LAND either individually or as part of an estate[9].

2.4 OpenSea

OpenSea is the largest cryptocurrency goods marketplace, specializing in NFTs and providing a wide range of crypto assets. They provide items in the following categories like virtual worlds, music, photography, sports, trading cards, collectibles, and domain names. Users can access, purchase, sell, and trade non-fungible tokens on OpenSea. The uniqueness of non-fungible tokens is that they cannot be exchanged for another item. In contrast to something like bitcoin, which is fungible and the same asset that you can exchange for another bitcoin[10]. With the help of the item minting tool from OpenSea, creators can produce their own goods on the blockchain. If users are selling products on OpenSea, users have the option of listing them for a set price, declining price, or auction[11]. When we talk about the limitations of the OpenSea, there is a Gas fee, takes time to set up a wallet and purchase ETH (Ethereum), high energy consumption, a maximum 10% royalty rate, does not take USD or Euro, difficult for artists to stand out and lack of advertising opportunities on the site[12].

The difference between this project with our one is that they are selling and buying virtual assets like graphics instead of real assets. But in our project, we are dealing with real physical assets (vehicles).

2.5 Summary

We have already outlined the preceding comparable projects. There are many limitations to those projects. In our project, when designing our project, we have solved a lot of these concerns and limitations which are mentioned blockchain-based vehicle registration and ownership management system. In contrast to the blockchain-based vehicle registration and ownership management system, non-fungible tokens (NFTs) are used to represent physical assets, such as vehicles. In contrast to the blockchain-based vehicle registration and ownership management system, non-fungible tokens (NFTs) are used to represent physical assets, such as vehicles. It is stored on a blockchain, which is a distributed ledger technology that allows for the secure and transparent tracking of transactions. The next chapter will focus on the technologies that we are using in our project and give an idea about how we are referring to these technologies to address our problem. To complete this project, we have to use many tools and technologies. In the next chapter, we are going to discuss these tools and technologies.

Chapter 3 Adapted Technologies

3.1 Introduction

There are many similar projects for our project. But there were many differences between those projects with our project from the used technologies point of view and the application's usage point of view. That's what we discussed in the last chapter. In this chapter, we will focus on the technologies that we are using in our project and give an idea about how we are referring to these technologies to address our problem. The current existing web browsers and web applications mostly support web 2.0. But we are going to do our project based on web 3. Therefore, we must use both web 2 and web 3 technologies and frameworks. In section 3.2 and section 3.3 we are descriptively discussing these technologies and how we refer to these technologies separately.

3.2 Web2

In terms of describing web 2.0, the phrase refers to online tools that let users collaborate and share with one another while also facilitating their online expression. It is only an upgraded version of the original worldwide web, distinguished particularly by the shift from static to dynamic or user-generated content as well as the expansion of social media. Rich web applications, web-oriented architecture, and social web are all mentioned in the Web 2.0 idea. Without any modifications to the technical standards, it refers to changes in the way web pages are designed and utilized by users[13].

In terms of describing web 2.0, the phrase refers to online tools that let users collaborate and share with one another while also facilitating their online expression. It is only an upgraded version of the original worldwide web, distinguished particularly by the shift from static to dynamic or user-generated content as well as the expansion of social media. Rich web applications, web-oriented architecture, and social web are all mentioned in the Web 2.0 idea. Without any modifications to the technical standards, it refers to changes in the way web pages are designed and utilized by users[13].

3.2.1 ReactJS

A straightforward, feature-rich, component-based JavaScript UI library is ReactJS. Both tiny and large, complicated applications can be created with it. It was created by Facebook. ReactJS offers a basic yet reliable feature set to get a web application off of the market. React community supports React library by offering a sizable collection of

pre-made components to quickly construct web applications. On top of the React library, the React community offers advanced concepts like state management, routing, etc. React has become a developer favorite and has become one of the most popular front-end frameworks[14]. NextJS is built on top of react. Therefore, to take the NextJS support we had to use ReactJS.

A straightforward, feature-rich, component-based JavaScript UI library is ReactJS. Both tiny and large, complicated applications can be created with it. It was created by Facebook. ReactJS offers a basic yet reliable feature set to get a web application off of the market. React community supports React library by offering a sizable collection of pre-made components to quickly construct web applications. On top of the React library, the React community offers advanced concepts like state management, routing, etc. React has become a developer favorite and has become one of the most popular front-end frameworks[14]. NextJS is built on top of react. Therefore, to take the NextJS support we had to use ReactJS.

3.2.2 React Native

A JavaScript framework called React Native is used to create native mobile applications. It was created by Facebook and is frequently used to create iOS and Android cross-platform mobile apps. Not only that but also can be used by windows, Linux, and mac OS. With React Native, mobile apps can be created of needing to maintain several codebases for each platform, developers can write code just once and reuse it for both.

The popular JavaScript library for designing user interfaces, React, is used by React Native. It enables the creation of reusable UI components, which can accelerate development and maintain a unified aesthetic across several platforms. Since React Native is open-source, developers can simply contribute to its development and advancement for free. It features a sizable and vibrant developer and user community that offers a plethora of information and assistance for creating mobile apps with React Native[15], [16]. In our SSI Mobile Wallet, we have to maintain different code bases for the same project. Therefore, we had to go for a hybrid system. For that, we had three choices to develop this system. Accordingly, Flutter, React Native and Xamarin were the suggestions. Our web based NFT marketplace uses React for the front end. React

and React Native are a bit similar and also the learning curve for React Native is less. Therefore, out of those choices, the most suitable one for our project is React Native.

The popular JavaScript library for designing user interfaces, React, is used by React Native. It enables the creation of reusable UI components, which can accelerate development and maintain a unified aesthetic across several platforms. Since React Native is open-source, developers can simply contribute to its development and advancement for free. It features a sizable and vibrant developer and user community that offers a plethora of information and assistance for creating mobile apps with React Native[15], [16]. In our SSI Mobile Wallet, we have to maintain different code bases for the same project. Therefore, we had to go for a hybrid system. For that, we had three choices to develop this system. Accordingly, Flutter, React Native and Xamarin were the suggestions. Our web based NFT marketplace uses React for the front end. React and React Native are a bit similar and also the learning curve for React Native is less. Therefore, out of those choices, the most suitable one for our project is React Native.

3.2.3 NextJS

NextJS is a JavaScript framework for building server-rendered and statically generated web applications. It is built on top of React, a popular JavaScript library for building user interfaces, and it is designed to make it easy for developers to create fast and reliable web applications. One of the main features of NextJS is its ability to automatically optimize the performance of a web application by server rendering the initial HTML and then serving it to the client. This can help to improve the loading times of a web application, especially on slower connections or devices. NextJS also offers a range of other features that can be useful for web developers, such as automatic code splitting, built-in CSS support, and easy deployment to various cloud platforms. It is a popular choice for building web applications because it is easy to use and provides a lot of functionality outside of the box[17].

There are four major reasons to use NextJS for our project. According to that server-side rendering, automatic code splitting, static exporting, and routing can be done easily using NextJS on top of ReactJS. And not only that to work with a blockchain there are supportive modules in NextJS like web3.js, Truffle, MetaMask, and Embark.

3.2.4 Django

Python-based backend server-side web application framework called Django is free and open source. It uses MVT design principles (MVT stands for Model View Template). In the current market, Django is really demanding because of its quick development capability. The development of any form of application requires less time[18].

When developing SSI Issuer and SSI verifier we use Django as the backend framework. Therefore, it is possible to handle a heavy request load. And this framework is very supportive and comfortable for rapid development. Django is a stable framework that has a big community.

3.2.5 PostgreSQL

PostgreSQL is a powerful, open-source object-relational database system with a strong reputation for reliability, feature robustness, and performance. It is a popular choice for web applications, data warehousing, and more. It is designed to handle a wide range of workloads, from single machines to data warehouses or Web services with many concurrent users. It is highly customizable, allowing users to write custom functions and extensions in a variety of languages[19]. We use PostgreSQL because of the Django is very supported for this database.

PostgreSQL is a powerful, open-source object-relational database system with a strong reputation for reliability, feature robustness, and performance. It is a popular choice for web applications, data warehousing, and more. It is designed to handle a wide range of workloads, from single machines to data warehouses or Web services with many concurrent users. It is highly customizable, allowing users to write custom functions and extensions in a variety of languages[19]. We use PostgreSQL because of the Django is very supported for this database.

3.3 Web3

Web3 refers to the third generation of the World Wide Web, which emphasizes the use of decentralized technologies such as blockchain and peer-to-peer networking to enable new applications and services. Web3 technologies have the potential to enable greater decentralization, security, and privacy on the web, and to create new opportunities for innovation and collaboration. Web3 technologies have the potential to disrupt a wide range of industries, including finance, supply chain management, voting systems, and more. They also have the potential to empower individuals and communities by giving

them greater control over their data and assets, and by enabling new forms of collaboration and decision-making[20].

Web3 refers to the third generation of the World Wide Web, which emphasizes the use of decentralized technologies such as blockchain and peer-to-peer networking to enable new applications and services. Web3 technologies have the potential to enable greater decentralization, security, and privacy on the web, and to create new opportunities for innovation and collaboration. Web3 technologies have the potential to disrupt a wide range of industries, including finance, supply chain management, voting systems, and more. They also have the potential to empower individuals and communities by giving them greater control over their data and assets, and by enabling new forms of collaboration and decision-making[20].

3.3.1 Blockchain

Blockchain is a decentralized, immutable database that makes it easier to track assets and record transactions in a corporate network. An asset may be physical (such as a home, car, money, or land) or intangible (intellectual property, patents, copyrights, branding). On a blockchain network, practically anything of value may be recorded and traded, lowering risk and increasing efficiency for all parties[21].

Blockchain is a decentralized, immutable database that makes it easier to track assets and record transactions in a corporate network. An asset may be physical (such as a home, car, money, or land) or intangible (intellectual property, patents, copyrights, branding). On a blockchain network, practically anything of value may be recorded and traded, lowering risk and increasing efficiency for all parties[21].

3.3.1.1 Indy Blockchain

The Hyperledger project created the open-source distributed ledger technology (DLT) platform known as Indy, which stands for "Independent Identity". It's intended to be a self-sovereign identity (SSI) solution that enables people and organizations to control their own identity data on a blockchain. Instead of being centrally managed by a single institution, identification information is maintained on a decentralized network of computers in an SSI system centered in Indianapolis. This enables people and organizations to exercise more control over and selective sharing of their own identity data. With the help of Indy, people and organizations may manage their digital identity

data in a safe and private manner. It can be used for many different purposes, such as data sharing, access control, and identity verification [22].

The Hyperledger project created the open-source distributed ledger technology (DLT) platform known as Indy, which stands for "Independent Identity". It's intended to be a self-sovereign identity (SSI) solution that enables people and organizations to control their own identity data on a blockchain. Instead of being centrally managed by a single institution, identification information is maintained on a decentralized network of computers in an SSI system centered in Indianapolis. This enables people and organizations to exercise more control over and selective sharing of their own identity data. With the help of Indy, people and organizations may manage their digital identity data in a safe and private manner. It can be used for many different purposes, such as data sharing, access control, and identity verification [22].

We need an identity management system that is according to the standard. The Indy blockchain is very stable and is supported by the BC government and the Linux foundation. It is better than using a custom identity management system. Therefore, we use Indy blockchain for our project. Issuing self-sovereign identity for the user and verification can be done by this blockchain.

3.3.1.2 Polygon Blockchain

To address Ethereum's scalability problems, a stack of protocols called Polygon was created. By managing transactions on a different Ethereum-compatible blockchain, the Polygon network resolves the network's issues. Transactions are then returned by Polygon for post-processing on the main Ethereum network. This strategy lessens the stress on Ethereum's network. Through this, Polygon can accelerate transactions and bring down transaction costs to just a penny. In other words, Polygon, formerly Matic network, offers a simple foundation for new and current blockchain projects to develop on Ethereum without scalability difficulties. Users that use Polygon never have to be concerned about network congestion when interacting with any decentralized application (DApp)[23].

To address Ethereum's scalability problems, a stack of protocols called Polygon was created. By managing transactions on a different Ethereum-compatible blockchain, the Polygon network resolves the network's issues. Transactions are then returned by

Polygon for post-processing on the main Ethereum network. This strategy lessens the stress on Ethereum's network. Through this, Polygon can accelerate transactions and bring down transaction costs to just a penny. In other words, Polygon, formerly Matic network, offers a simple foundation for new and current blockchain projects to develop on Ethereum without scalability difficulties. Users that use Polygon never have to be concerned about network congestion when interacting with any decentralized application (DApp)[23].

We have two choices to write smart contract/ chain codes. Those are hypogene fabric and Ethereum 2.0. The hypogene fabric is less supportive compared to Ethereum. Therefore, we tried Ethereum. Then we have two choices between normal Ethereum and polygon blockchain. Both of these are based on Ethereum. Therefore, there is no issue with technology and security. But we chose Polygon as it is cost-effective.

3.3.1.3 IPFS Blockchain

Inter Planetary File System (IPFS), a peer-to-peer (P2P) hypermedia protocol, was introduced in an effort to bring about a new internet revolution. Users may store and access data including files, programs, and webpages thanks to this distributed infrastructure. The bigger goal of IPFS is to build a global computer network that ensures censorship-resistant, private, and secure connectivity[24]. In our project we have to save our related files. It is not secure to save these files in the local server. Therefore, we are using IPFS blockchain.

Inter Planetary File System (IPFS), a peer-to-peer (P2P) hypermedia protocol, was introduced in an effort to bring about a new internet revolution. Users may store and access data including files, programs, and webpages thanks to this distributed infrastructure. The bigger goal of IPFS is to build a global computer network that ensures censorship-resistant, private, and secure connectivity[24]. In our project we have to save our related files. It is not secure to save these files in the local server. Therefore, we are using IPFS blockchain.

3.3.2 Aries Cloud Agent - Python

Developers can easily create decentralized identity services that leverage verifiable credentials using the flexible, extensible, non-mobile Aries agent known as Aries Cloud Agent Python (ACA-Py). ACA-Py is used as an interface to a legacy system to issue verifiable credentials, an authentication service based on the presentation of verifiable

credential proofs, an enterprise wallet to hold and present verifiable credentials about that enterprise, and a user interface for a person to use a wallet not stored on a mobile device[25].

We use polygon blockchain to communicate with the Indy blockchain. It is very hard to use SDK of Indy blockchain as it has some bugs. Therefore, we use ACA-Py to communicate with the Indy blockchain.

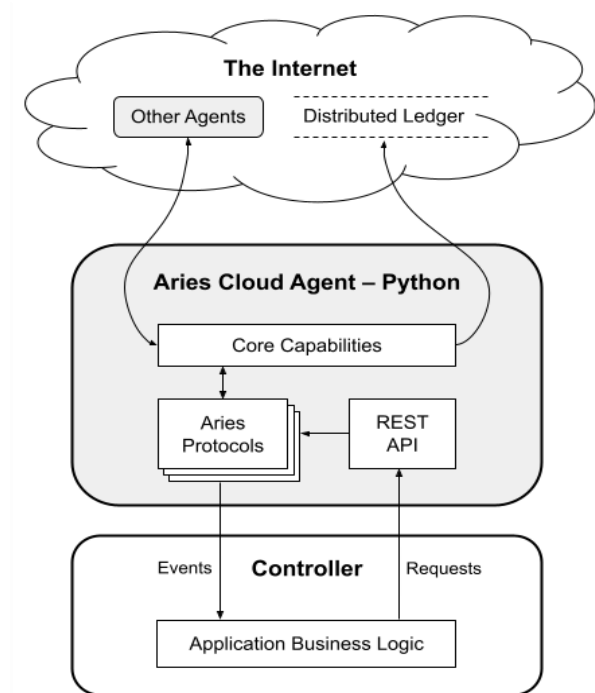


Figure 3-1 Overview of the Architecture of the Aries Cloud Agent - Python

3.3.3 MetaMask Wallet

Several different Ethereum-based tokens and non-fungible tokens (NFTs) are supported by the well-known cryptocurrency wallet MetaMask on supported blockchains. While seasoned cryptocurrency investors would value the wallet's speed and simplicity, novice investors might find it challenging to use. A deterrent for investors whose primary investment is Bitcoin is the wallet's lack of support for Bitcoin[26]

A digital wallet and browser extension called MetaMask use to communicate with the Ethereum network. This application can be used to connect with decentralized applications (dApps) created on the Ethereum platform as well as store, manage, and use users' Ether (ETH) and other Ethereum-based assets.

With MetaMask it is possible to manage Ethereum assets and accounts, as well as sign and send transactions on the Ethereum network. As a result, you can use application

features and services without having to install them locally on your computer by interacting with them in your browser. We use MetaMask to do the transactions with Ethereum. Generally, MetaMask wallet is the easiest way to do the transactions with Ethereum.

3.4 Docker

Docker is a tool designed to make it easier to create, deploy, and run applications by using containers. A container is a lightweight, stand-alone, and executable package that includes everything an application needs to run, such as code, libraries, dependencies, and runtime. Docker provides a way to create and manage containers, allowing developers to focus on writing and deploying their applications, rather than spending time on the underlying infrastructure. Docker also provides a platform for sharing and distributing containerized applications, through a registry called Docker Hub[27] When we are installing Aries cloud python on our local machine, we have to face dependency errors. For the purpose of solving this error, Aries Cloud Python (ACA py) has been introduced officially to docker.

Docker is a tool designed to make it easier to create, deploy, and run applications by using containers. A container is a lightweight, stand-alone, and executable package that includes everything an application needs to run, such as code, libraries, dependencies, and runtime. Docker provides a way to create and manage containers, allowing developers to focus on writing and deploying their applications, rather than spending time on the underlying infrastructure. Docker also provides a platform for sharing and distributing containerized applications, through a registry called Docker Hub[27] When we are installing Aries cloud python on our local machine, we have to face dependency errors. For the purpose of solving this error, Aries Cloud Python (ACA py) has been introduced officially to docker.

3.4.1 Docker Compose

Docker Compose is a tool for defining and running multi-container Docker applications. It allows developers to use a YAML file to define the structure and configuration of their application's services, and then use a single command to create and start all of the services from their configuration. Overall, Docker Compose is a useful tool for developers who are working with multi-container applications, as it

provides a way to define and manage the components and their dependencies in a simple and consistent manner[28].

Docker Compose is a tool for defining and running multi-container Docker applications. It allows developers to use a YAML file to define the structure and configuration of their application's services, and then use a single command to create and start all of the services from their configuration. Overall, Docker Compose is a useful tool for developers who are working with multi-container applications, as it provides a way to define and manage the components and their dependencies in a simple and consistent manner[28].

3.5 Summary

We have already outlined the technologies which are used in our project and how we are referring to those technologies to address our problem in this chapter. Those are web2; ReactJS, React Native, NextJS, Django, and Blockchain; Indy, Polygon, IPFS, and Aries Cloud Agent- Python, Mets Mask Wallet, Docker, and Docker compose. In the next chapter we will discuss our proposed solution, who are the users, what are the activities they have done, what are the inputs and outputs and how we process to achieve our goal, and the software process model that we used to define and organize the activities and tasks involved in the development of our project. By using these technologies mentioned above how are we going to address our problem mentioned in the first chapter will be discussed in the next chapter.

Chapter 4 Our Approach

4.1 Introduction

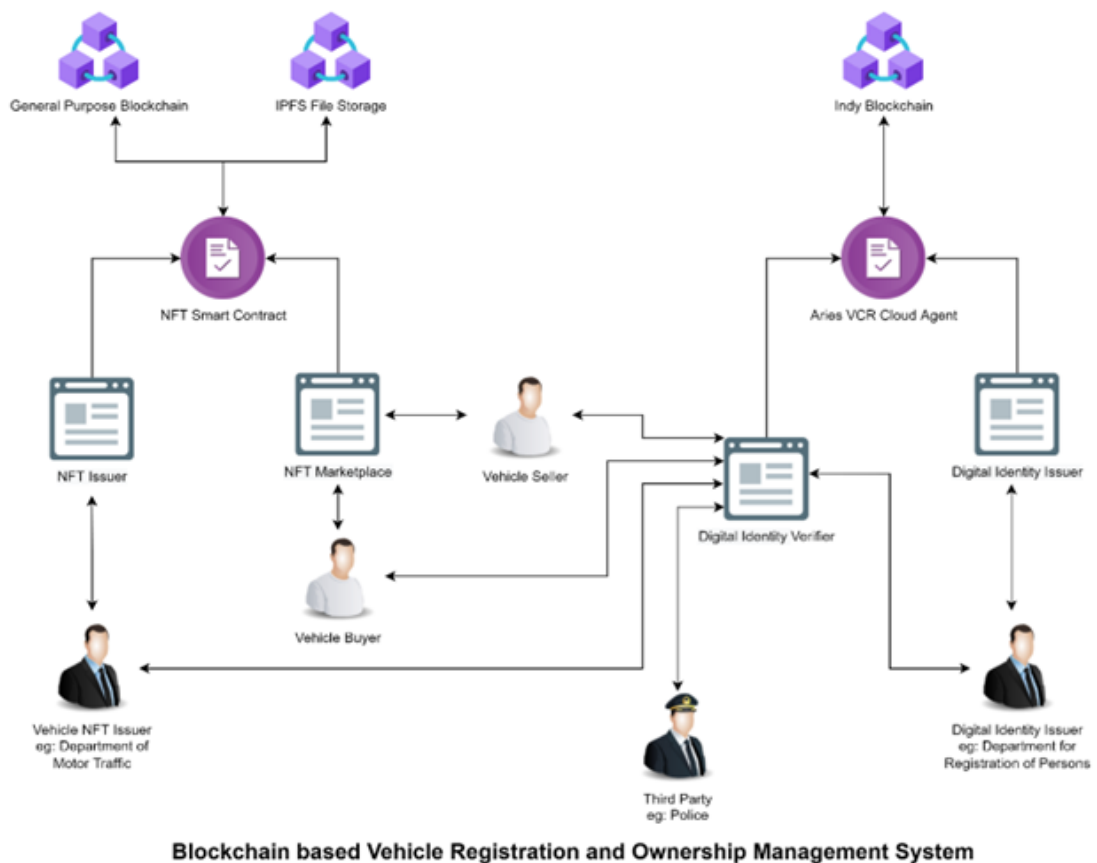
In the previous chapter, the technology adapted to our project was mentioned. In this chapter, we are going to discuss our proposed solution, who are the users of our system, what are the inputs and outputs and how we process to achieve our goal, and the software process model that we used to define and organize the activities and tasks involved in the development of our project. The Vehicle Registration and Ownership Management System is an application that facilitates digitizing the system of registering and transferring vehicle ownership with the use of Blockchain technology and NFTs are used for representing the vehicles. Users who want to sell or buy vehicles in a secure manner can use this application.

4.2 Blockchain-Based Vehicle Registration and Ownership Management System

Our main intention of the project is to digitize the registration and ownership management system of vehicles. We want to implement our system with security and transparency, as security is the most required factor in these kinds of systems. Therefore, it is not much better to use a centralized database, and therefore as the best way, we use a blockchain. The main task of our system is to convert a physical asset into a digital asset. As an example, in our system we convert vehicle asset into a NFT (Non-Fungible Token).

As we talk about the legal side of the vehicle, first we have to register it in a government affiliated institution. If we sell or buy registered vehicle, we have to transfer the legal owner ship properly. we can track all the important information such as transfer date of the vehicle, the owner after transferring the ownership of the vehicle in a super secure manner with this system. There is a special process that happened in registering the vehicle. When we are registering the vehicle, we can mint (create) NFT with all details of the vehicle. According to that, there can be photographs of the vehicle according to the standards, and also all the information related to the vehicle which are included in the scanned copy of vehicle registration book. Not only that, but also, we create a vehicle marketplace to provide the facility of selling and buying vehicles. In this process, transferring the ownership of the vehicle happens through the NFT. When the

lifetime of the vehicle is over, we have to remove the vehicle of use. In that case we can burn-out related NFT. But the information related to that NFT will remain forever with that blockchain. In the current situation, we have to identify a person legally on the internet. But there is not a proper way to show a person's digital identity. That means a person can't be legally identified in internet. Because of that we have to issue a digital verifiable ID for them. As we can identify the vehicle owner through this digital verifiable ID, we can use this ID to login the digital marketplace.



4.3 Users, Inputs, Outputs of the System

In our system, there are six users as General user, SSI issuing officer, Seller, Buyer, Vehicle owner, and NFT minting officer. The inputs of the Vehicle Ownership Management System are SSI as login credentials, NFT requesting form, NFT selling request, payment and NFT details which are related to the buying a vehicle, SSI creating form.

General user inputs SSI as the login credentials. Then the VOMS save the SSI. SSI issuing officer submits the SSI creating form as the input to the VOMS. The seller input

the NFT selling request to the VOMS. The buyer inputs the payment and NFT details which are related to the buying process to the VOMS. The VOMS outputs the NFT details to the buyer. NFT minter submit the NFT requesting form to the VOMS. And the VOMS outputs NFT address to the NFT minting officer.

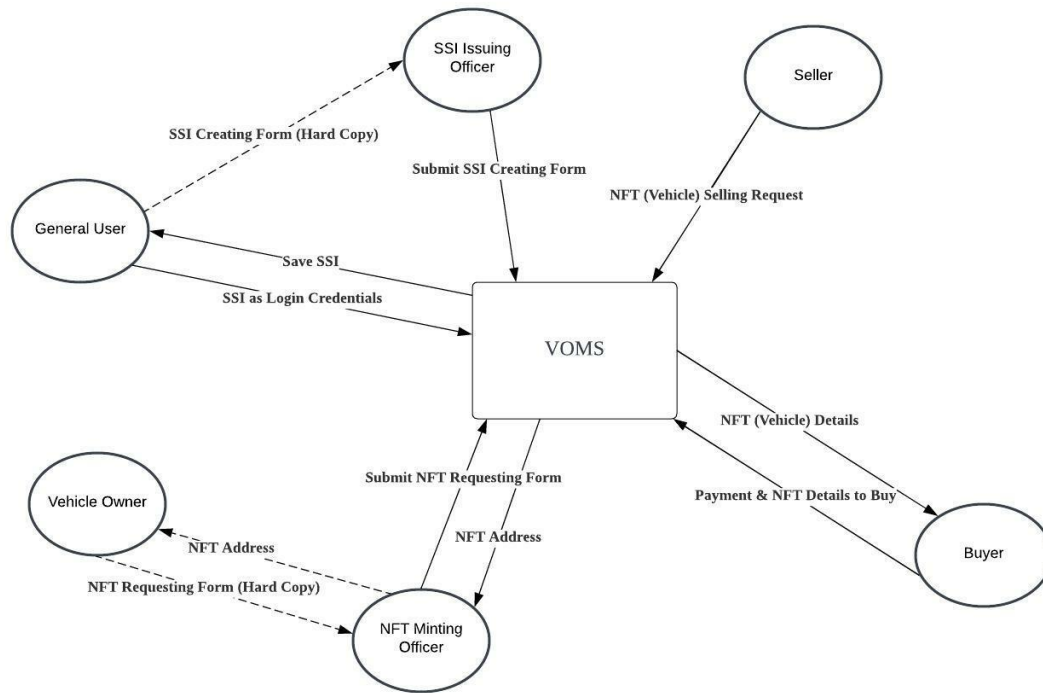


Figure 4-1 User, Input, Output Diagram

4.4 Systems Working Behavior

In this whole system there are mainly five parts. Those parts are the SSI Issuer, SSI Verifier, NFT Minter, NFT Vehicle selling and Buying Market Place and the SSI Wallet.

First if any person needs to sell or buy a vehicle, he or she must have an SSI to login to vehicle buying and selling marketplace. General users should give a hard copy of SSI request form to SSI issuing officer. Then SSI issuing officer log into the SSI issuer application. SSI issuing officer enters user's details into the SSI issuer application which is included in the SSI requesting form. After validating these data SSI issuing officer submit the form. Then these details were saved in the Postgres database in SSI Issuing application. SSI issuer sends an email to that user's email account which user provided to the SSI issuing officer. This email includes a link. When the general user

clicked that link it will generate a QR code. Then the general user should scan this generated QR code through his mobile SSI wallet. After scanning that QR code, mobile SSI wallet establishes a connection between SSI issuer and mobile SSI wallet through HTTP requests. Then SSI issuer pass the credential through Indy blockchain to the mobile SSI wallet.

When a vehicle owner wants to sell a vehicle through the marketplace, he or she want to get a NFT which represent their vehicle. To do that firstly the vehicle owner should give a hard copy of NFT requesting form. Then NFT minting officer log into the NFT minter application. NFT minting officer enters vehicle's details into the NFT minter application which is included in the NFT request form. At the same time NFT minting officer does a manual verification about provided details. As a further development, we can also add a verification with the database maintained by the government with vehicle details. After that, the NFT minting officer submits the form. The NFT is then minted in the polygon blockchain. After that, ownership of the NFT is transferred to the owner who the NFT requested within the polygon blockchain. This is the NFT minting process.

When a general user wants to buy or sell a vehicle, he or she wants to go to the marketplace. After the general user went to the marketplace there is a QR code which linked with an invitation. Then the user should scan this QR code from his mobile SSI wallet. After scanning that QR code, the mobile SSI wallet establishes a connection between the NFT marketplace and the mobile SSI wallet. Then the mobile SSI wallet presents the relevant credentials from its side. Now the NFT marketplace gets that credential through the mobile SSI wallet with the help of HTTP requests. Then these credentials are verified through the SSI verifier. If this credential has been verified, then user can log into the NFT marketplace. If credentials do not verify through the SSI verifier, then we can consider that user as an invalid user.

After logging to the NFT marketplace, if user is a seller and he or she wants to open a request to sell his vehicle, then the NFT of this vehicle is marked as sale. If the user is a buyer, then he can see all NFTs which are in the selling state with the price. After clicking a NFT which that buyer wants to buy, then the buyer can see all details such as who is created the NFT, how transfer ownerships etc. These details are immutable. Anyone cannot change it. After the buyer confirmed his buying, transaction will happen

through the MetaMask wallet to the polygon blockchain. Related payment will transfer to the smart contract. Then the ownership of the NFT will transfer to the buyer. After that a commission will be paid to the system's owner and the remaining amount will be transferred to the seller's account.

4.5 Software Process Model

Our project is given by the company called "Crede Technologies". When they provided this project to us, all the requirements were clarified correctly and clearly. Therefore, there was nothing to clarify in the software requirements. All the requirements were clear enough to give a full idea of the whole project. And also, we were provided with a tight deadline to complete this project. As a team, we have to complete tasks one by one instead of doing those activities concurrently. Our project development team does not consist of professionals and therefore most of the work is done as a team, instead of doing things individually. And also, we have a learning curve to follow. That's why the incremental model is not that handy to use for this project. And also, it is hard to communicate with our customers regularly. Therefore, the prototyping model is not suitable for this project. As system requirements are clear and there are no changing requirements, we do need a not agile approach. Considering all these facts and due to the correct and clear SRS, which is provided by the company, it is better to use the waterfall model as the software process model.

4.6 Summary

In this chapter, we already outlined our proposed solution, the users, what are the inputs and outputs and how we process to achieve our goal, and the software process model that we used to define and organize the activities and tasks involved in the development of our project. And also mentioned the software process model as the "Waterfall Model" which is used to develop our project. The next chapter will discuss the analysis and design of the project.

Chapter 5 Analysis and Design

5.1 Introduction

In chapter 4, the description with reference to users, inputs, outputs, process, technology that implements the solution were discussed. In this chapter, we gathered the requirements of the client and started to design the system after identifying the issue. At first, UML diagrams were designed for ease of understanding the system better. After Activity, Class and Sequence diagrams were designed to further understanding.

5.2 Analysis

Before designing the system, we identified the functional and non-functional requirements in the system as our client mentioned. The functional and non-functional requirements are mentioned in the SRS document.

5.3 Design

In this chapter, we will focus on the diagrams that we designed to visualize the functional and non-functional requirements. We have used Lucid Chart to draw the diagrams. There are several UML diagrams we have used,

1. Use case Diagram
2. Activity Diagram
3. Class Diagram
4. Sequence Diagram
5. ER Diagram

5.3.1 Use case Diagram

A use case diagram at its least difficult is a representation of a user's collaboration with the system that shows the connection between the user and the diverse use cases in which the user is included.

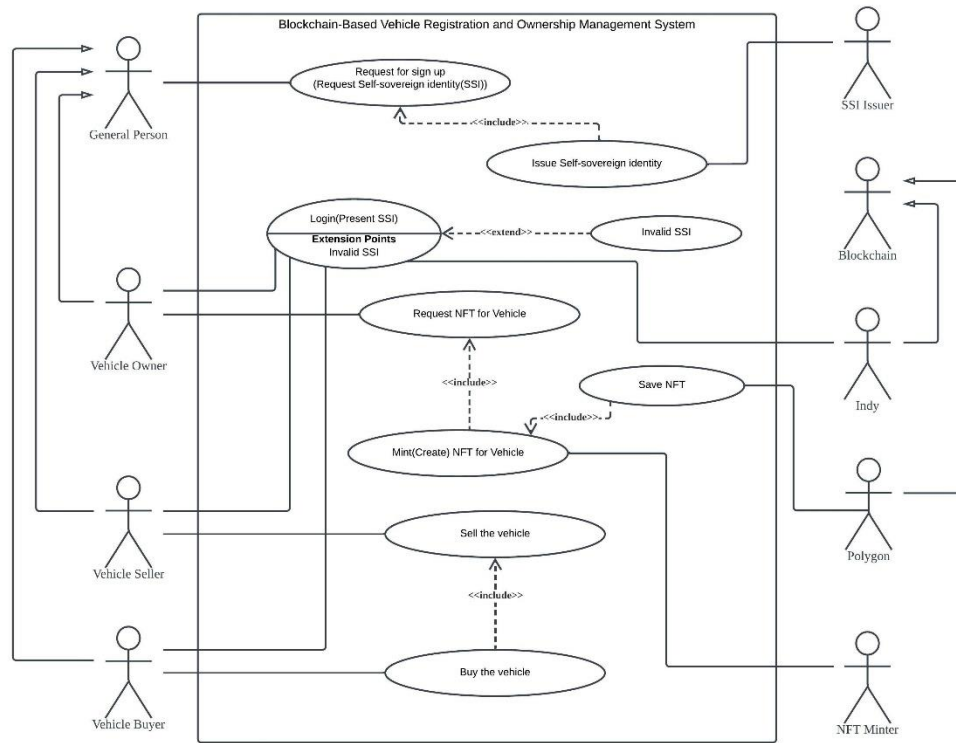


Figure 5-1 Use case Diagram

5.3.2 Activity Diagram

We created several activity diagrams to demonstrate some of the major activities in our system.

- SSI Issuer
- SSI Verifier
- Mobile SSI Wallet
- NFT Minter
- NFT Marketplace

5.3.2.1 SSI Issuer

First, we have to identify a user before he/ she enter to the marketplace. So, user should get their SSI. Then user can verify their own identity to our system. For that user should be fill the SSI creation form. And it will be submitted by the authorized office. Then it goes through multiple verifications processes and finally it issues and SSI directly to the user's wallet.

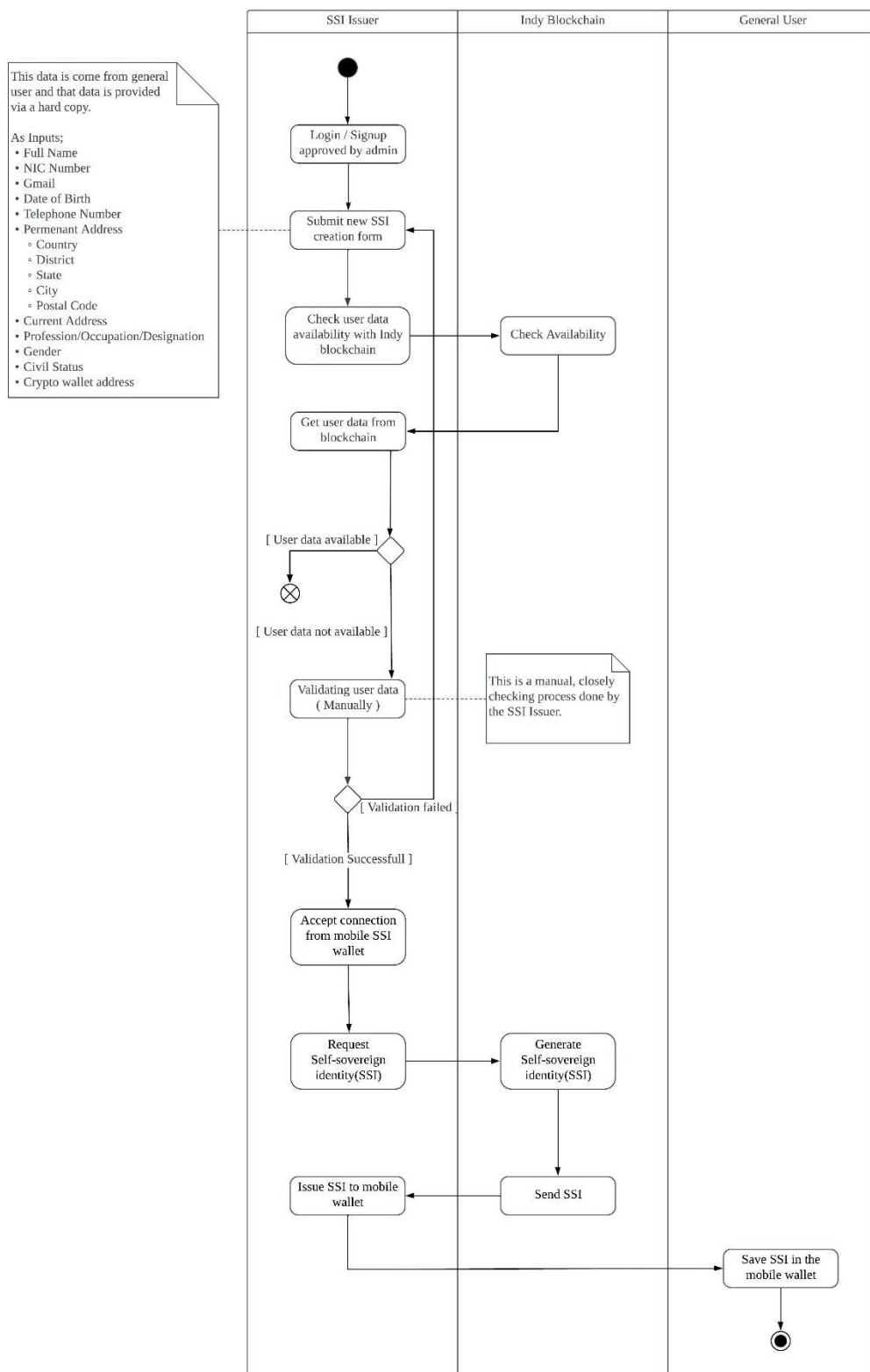


Figure 5-2 Activity Diagram of Issuing SSI process

5.3.2.2 SSI Verifier

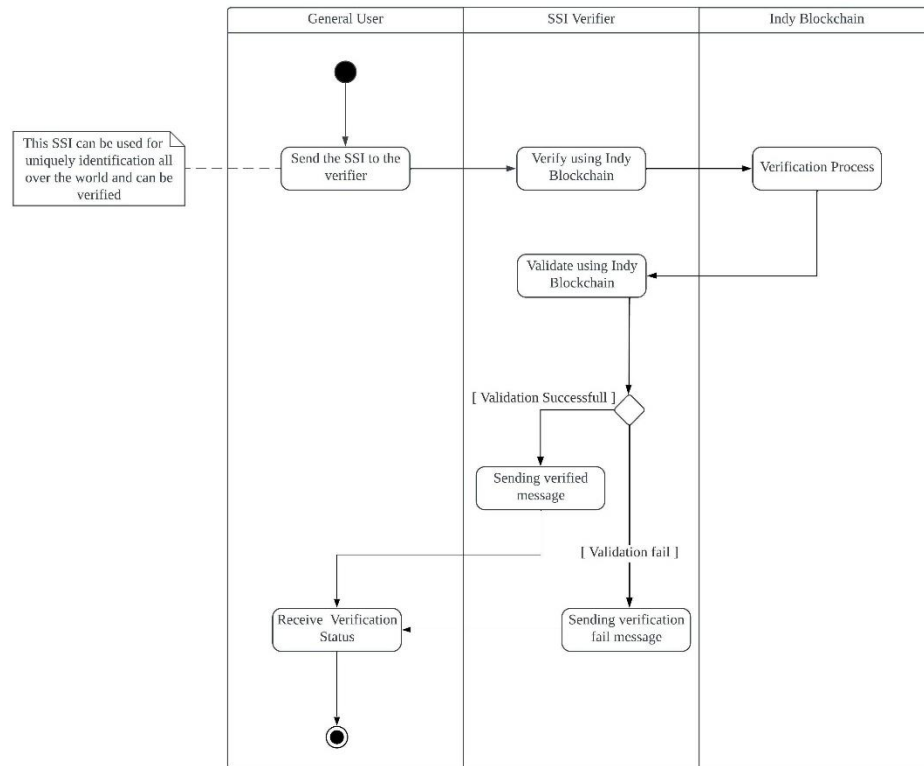


Figure 5-3 Activity Diagram Verifying SSI Process

5.3.2.3 Mobile SSI Wallet

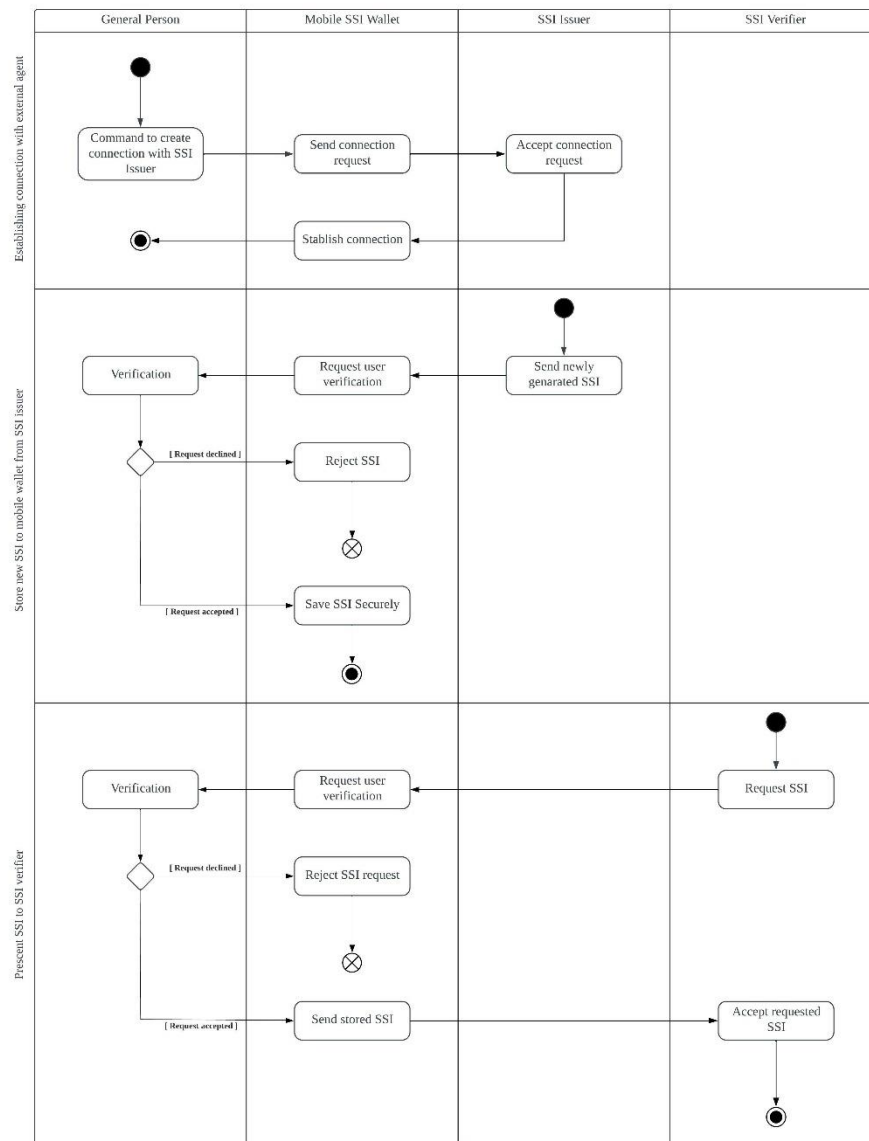


Figure 5-4 Activity Diagram saving newly created SSI

5.3.2.4 NFT Marketplace

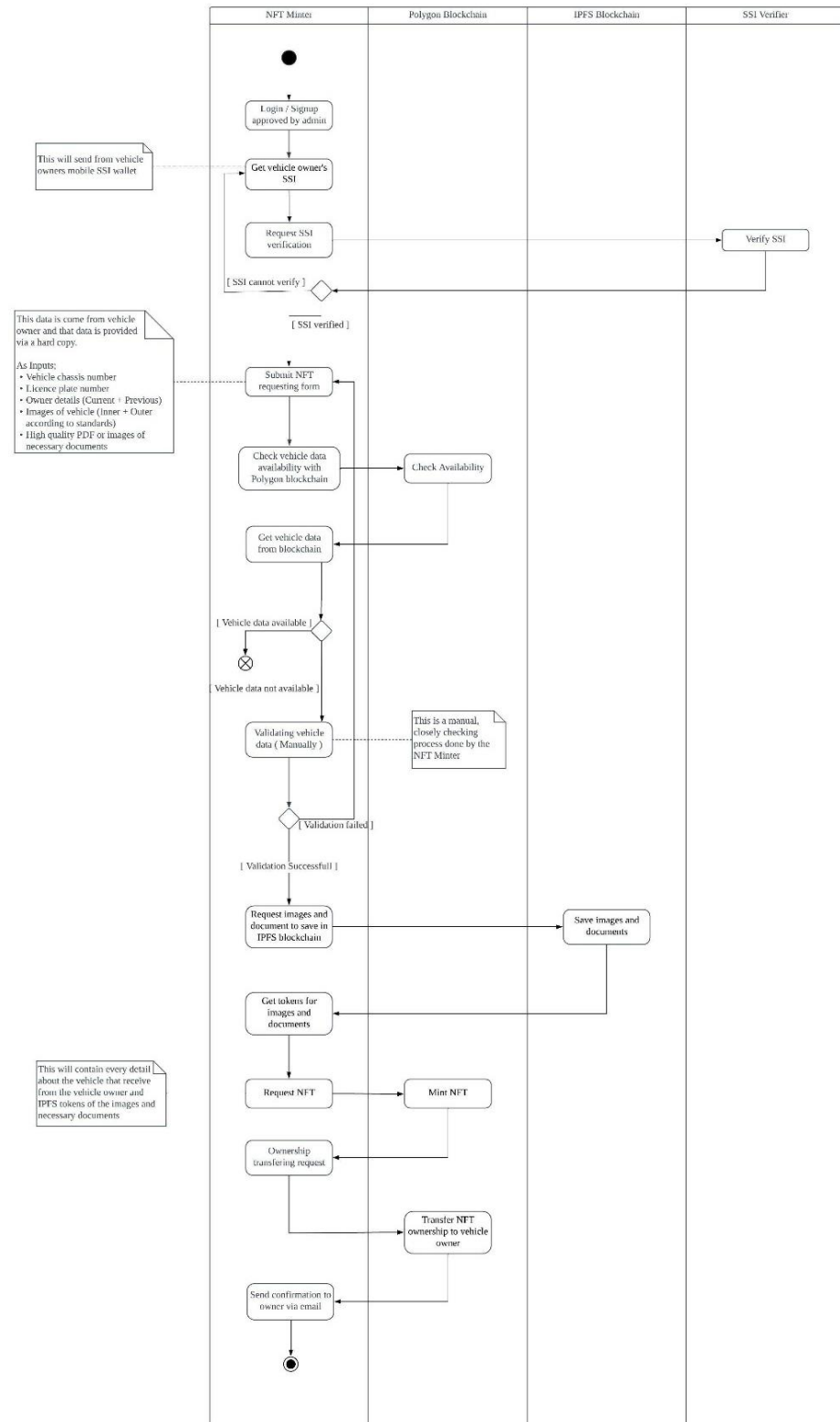


Figure 5-5 Minting NFT for Vehicle

5.3.2.5 NFT Marketplace

To sell vehicle

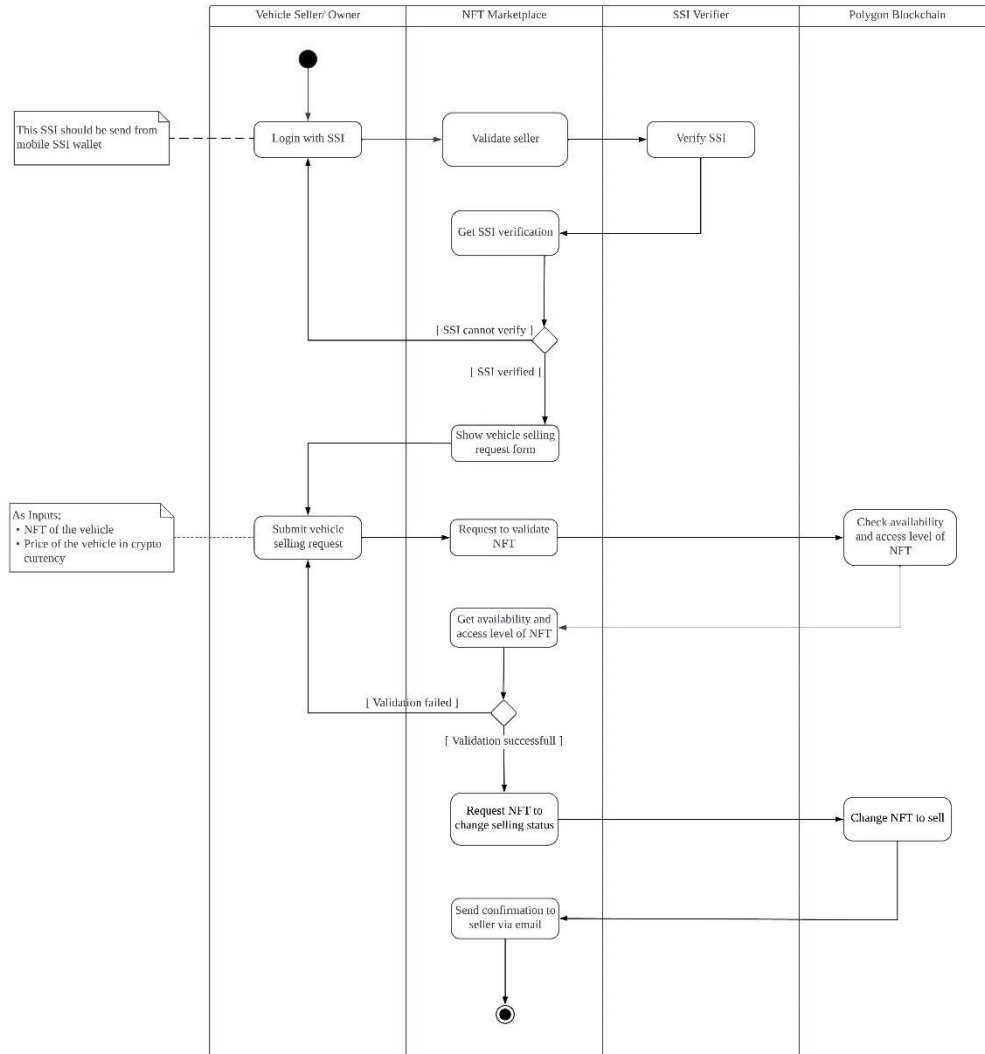


Figure 5-6 Activity Diagram NFT Market Place to sell vehicle

To buy vehicle

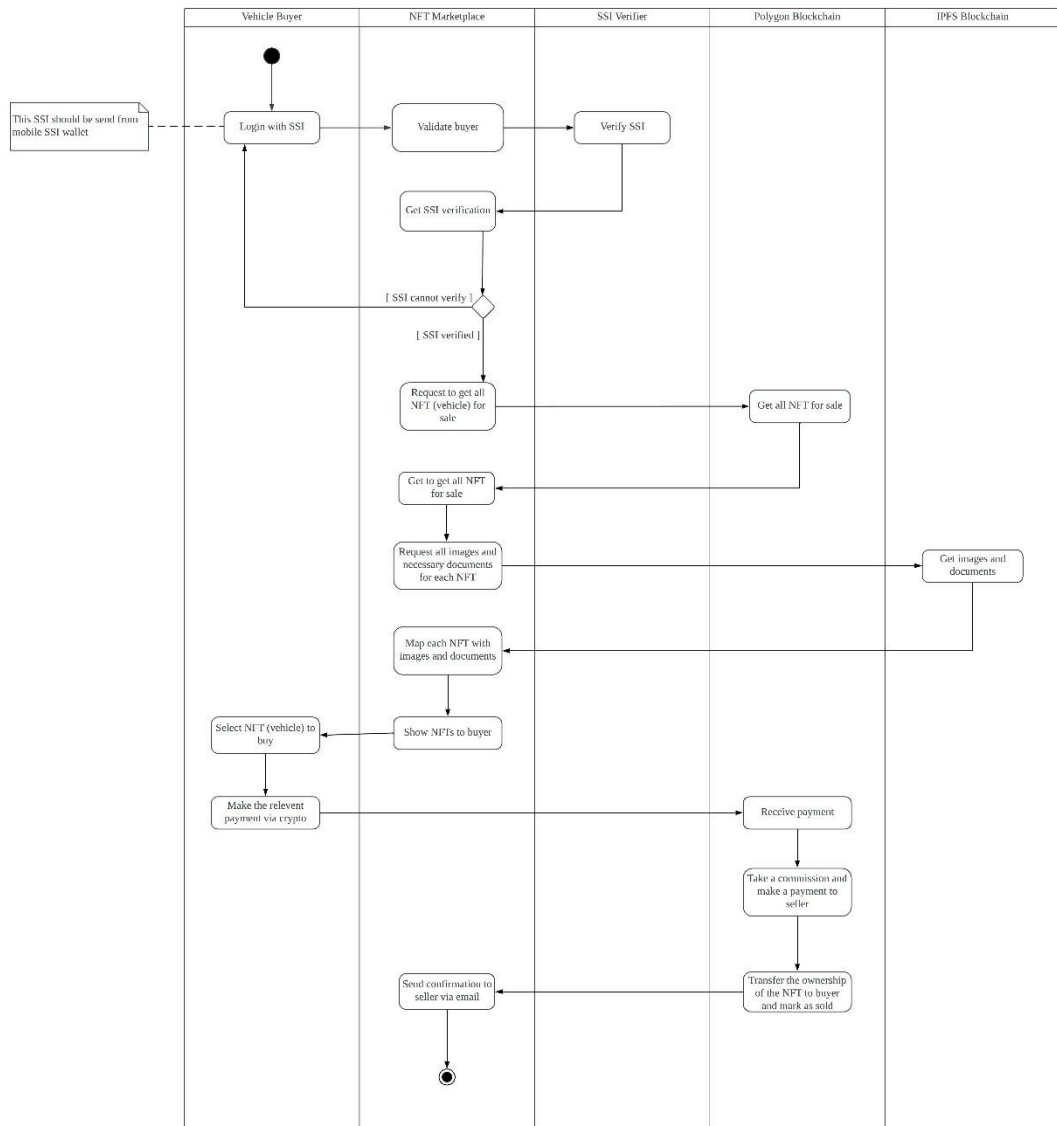


Figure 5-7 Activity Diagram NFT Market Place to buy vehicle

5.3.3 Class Diagram

A class diagram is a sort of static structure diagram that portrays the structure of a system by demonstrating the system's classes, their properties, methods and the relationship among objects.

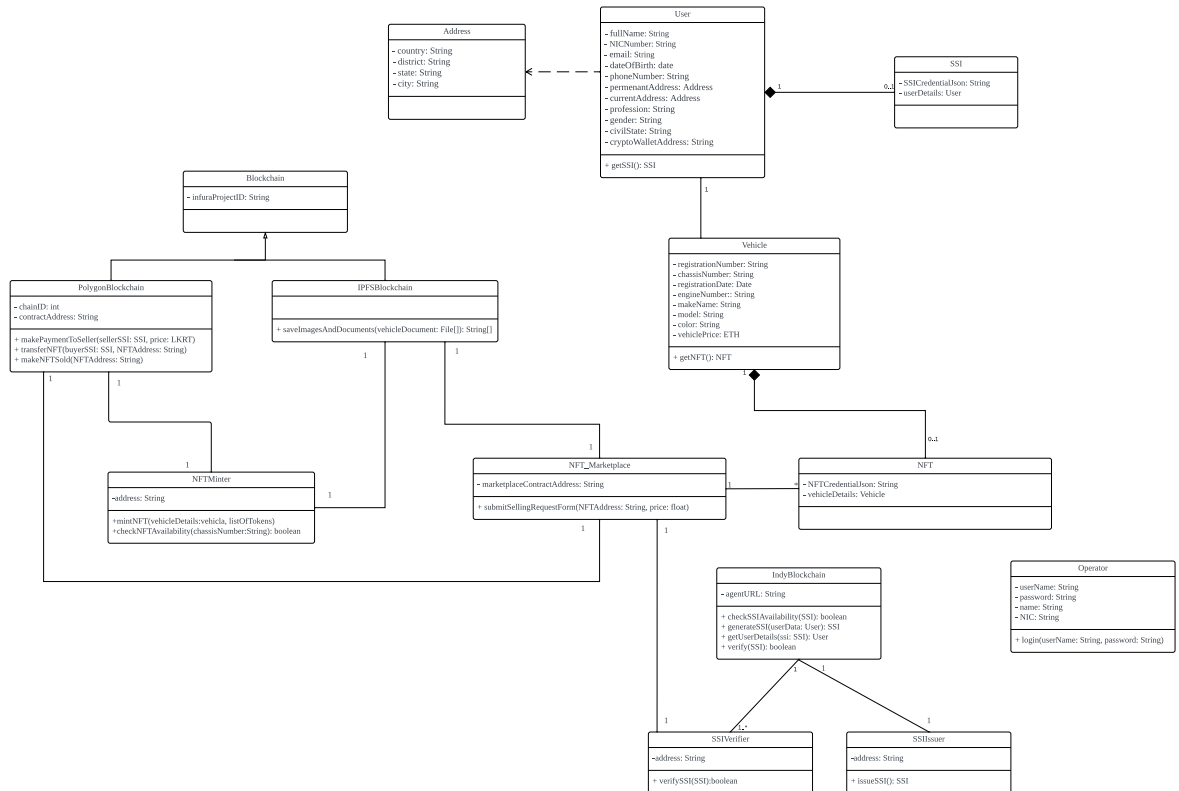


Figure 5-8 Class Diagram

5.3.4 Sequence Diagram

A sequence diagram shows object connections organized in time sequence. It demonstrates the objects associated with the scenario and the sequence of messages exchanged between the objects expected to complete the usefulness of the scenario. We designed several sequence diagrams as illustrated above.

5.3.4.1 Issuing SSI process

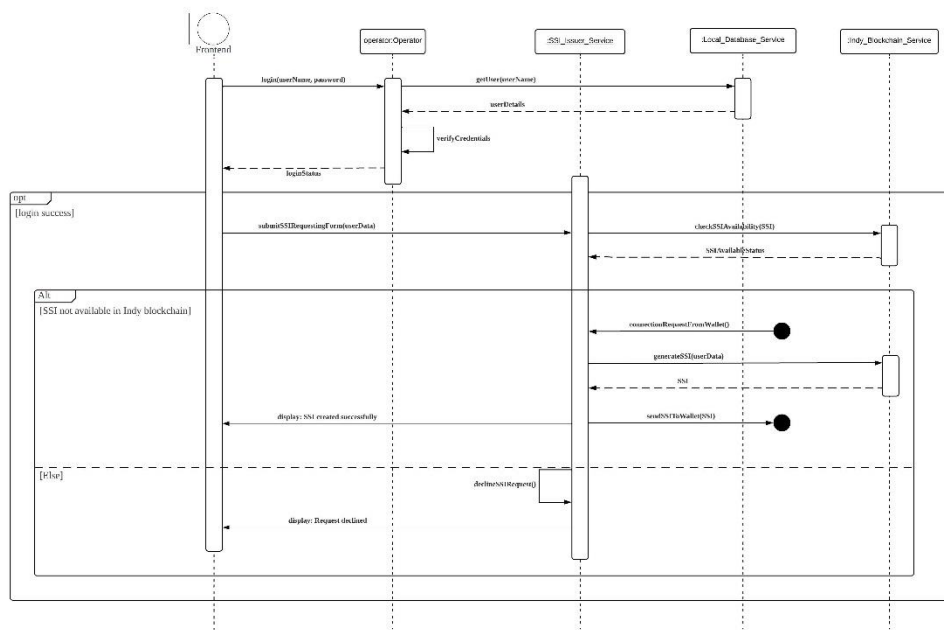


Figure 5-9 Sequence Diagram SSI Issuer

5.3.4.2 Verifying SSI process

Verify SSI via Web UI

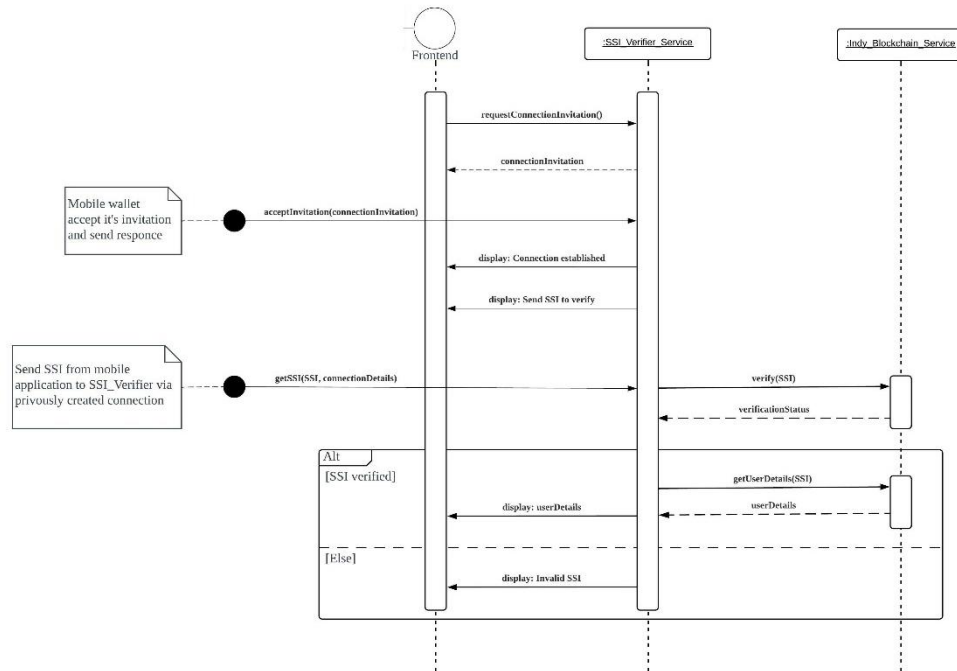


Figure 5-10 Sequence Diagram SSI Verifier (Web UI)

Verify SSI via API

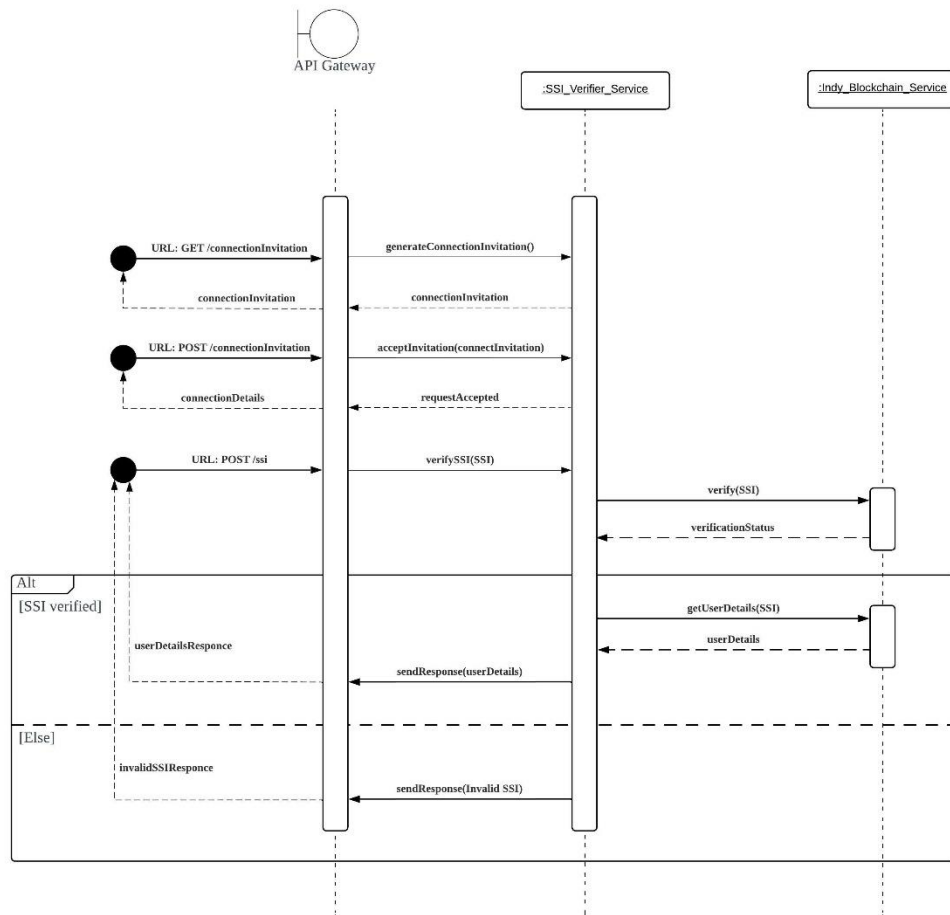


Figure 5-11 Sequence Diagram SSI Verifier (via API)

5.3.4.3 Saving Newly Created SSI

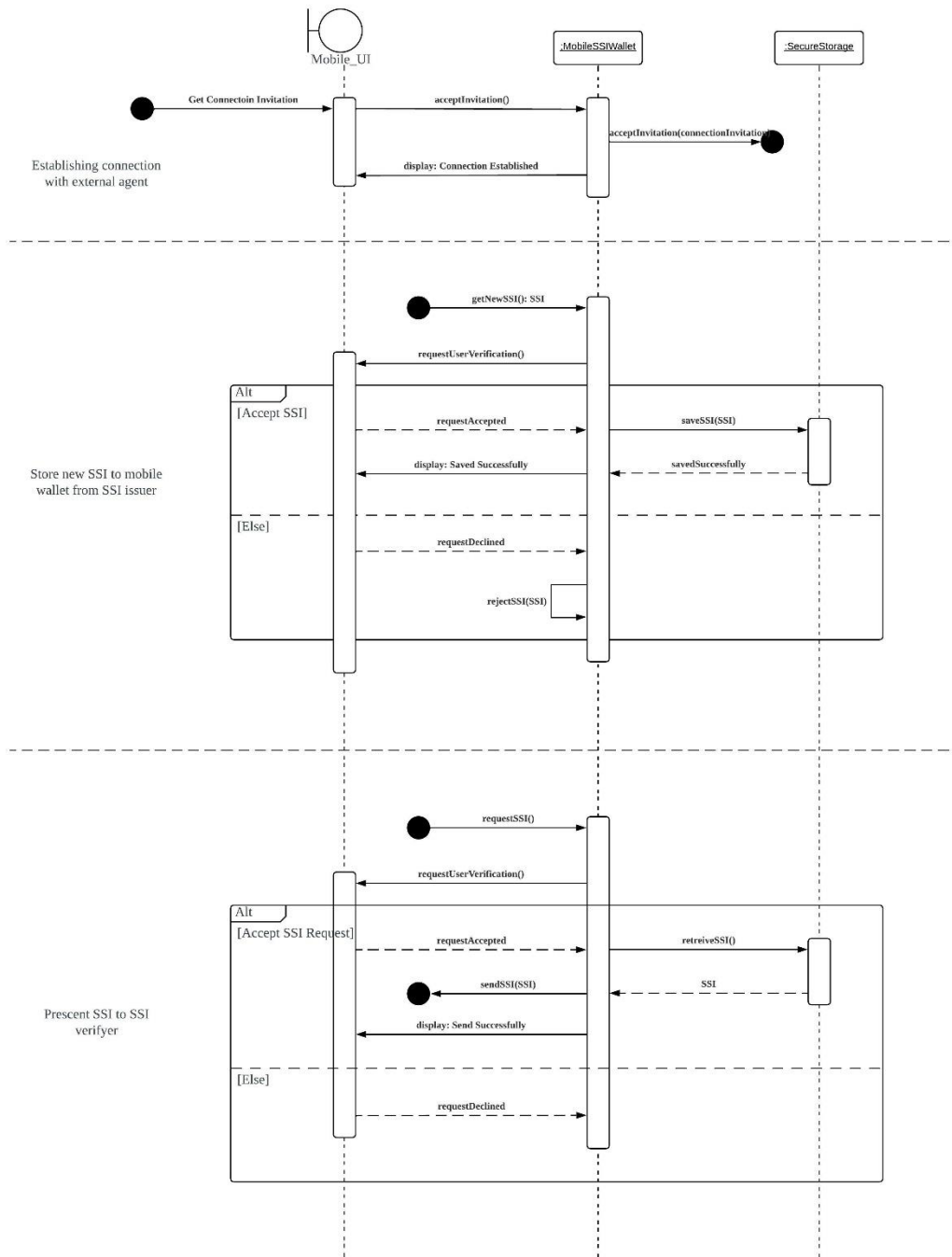


Figure 5-12 Sequence Diagram Mobile SSI Wallet

5.3.4.4 Minting NFT for Vehicle

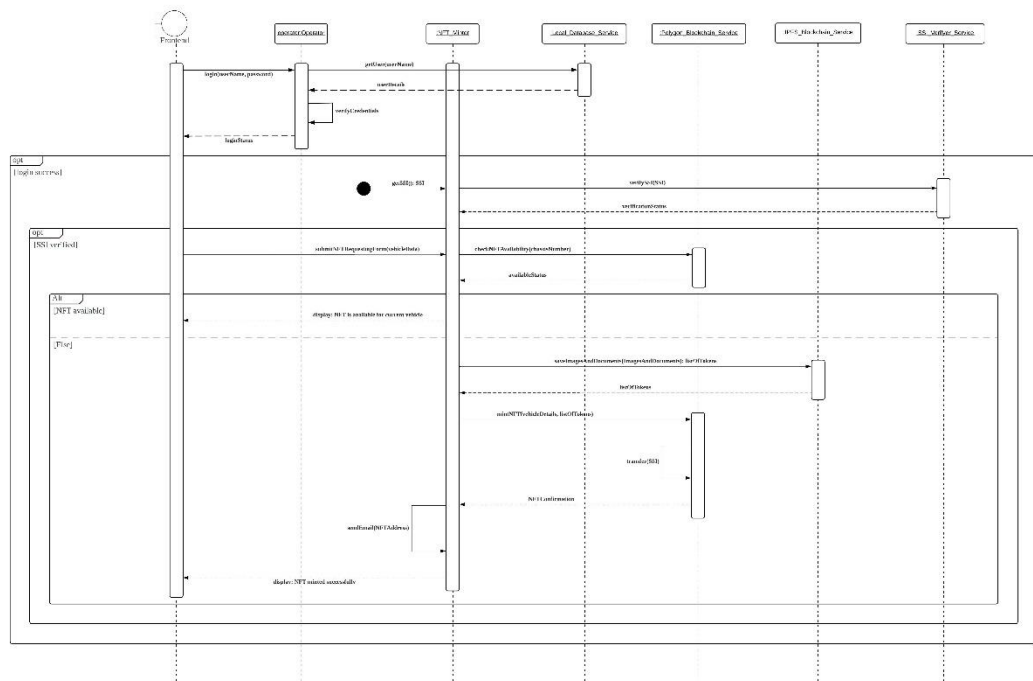


Figure 5-13 Sequence Diagram NFT Minter

5.3.4.5 Buying and Selling Vehicle in a Marketplace

Login with SSI

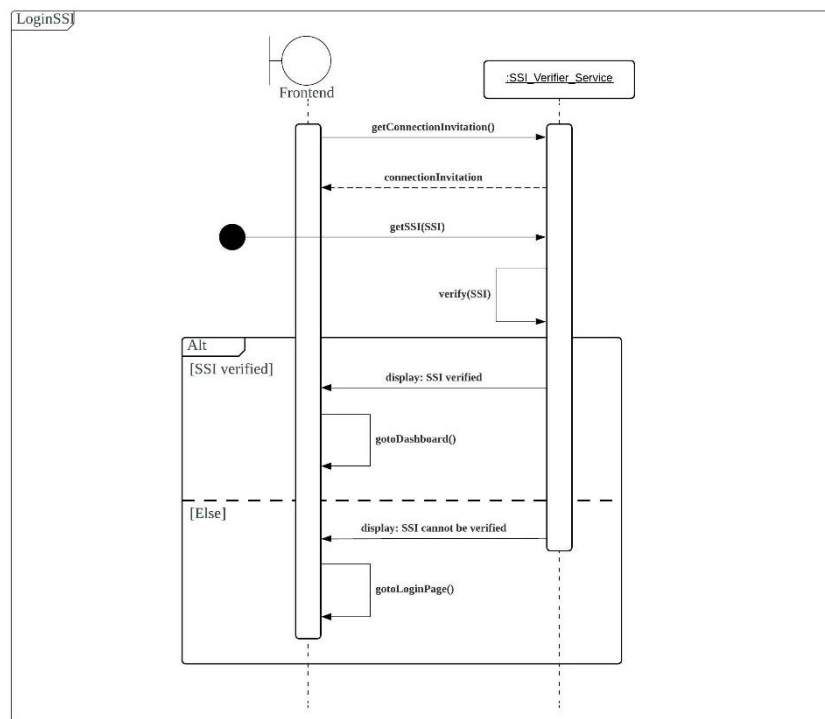


Figure 5-14 Sequence Diagram NFT Market Place (Login with SSI)

To Sell a Vehicle

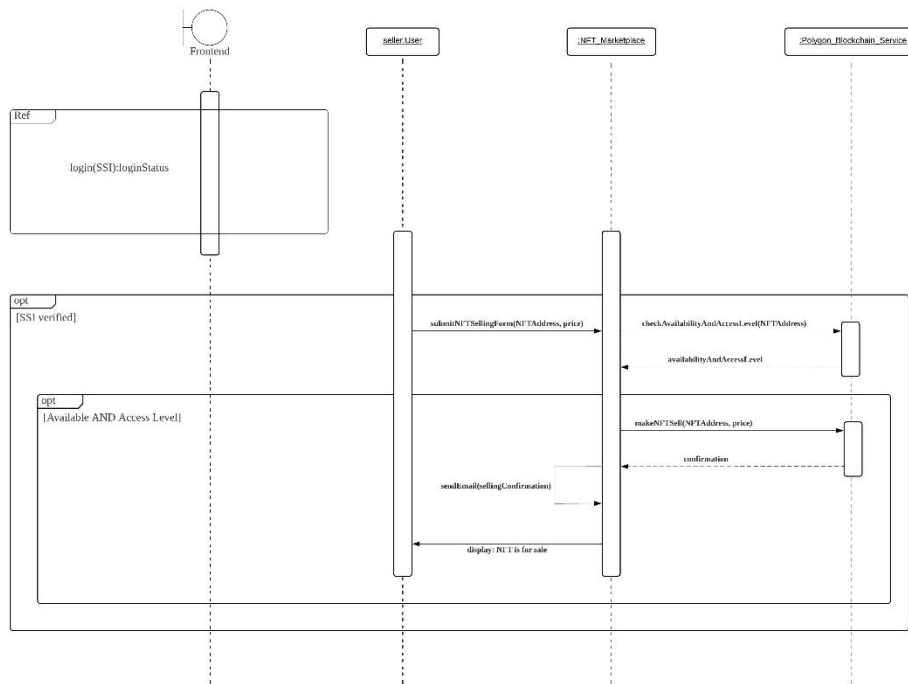


Figure 5-16 Sequence Diagram NFT Market Place (to sell a vehicle)

To Buy a Vehicle

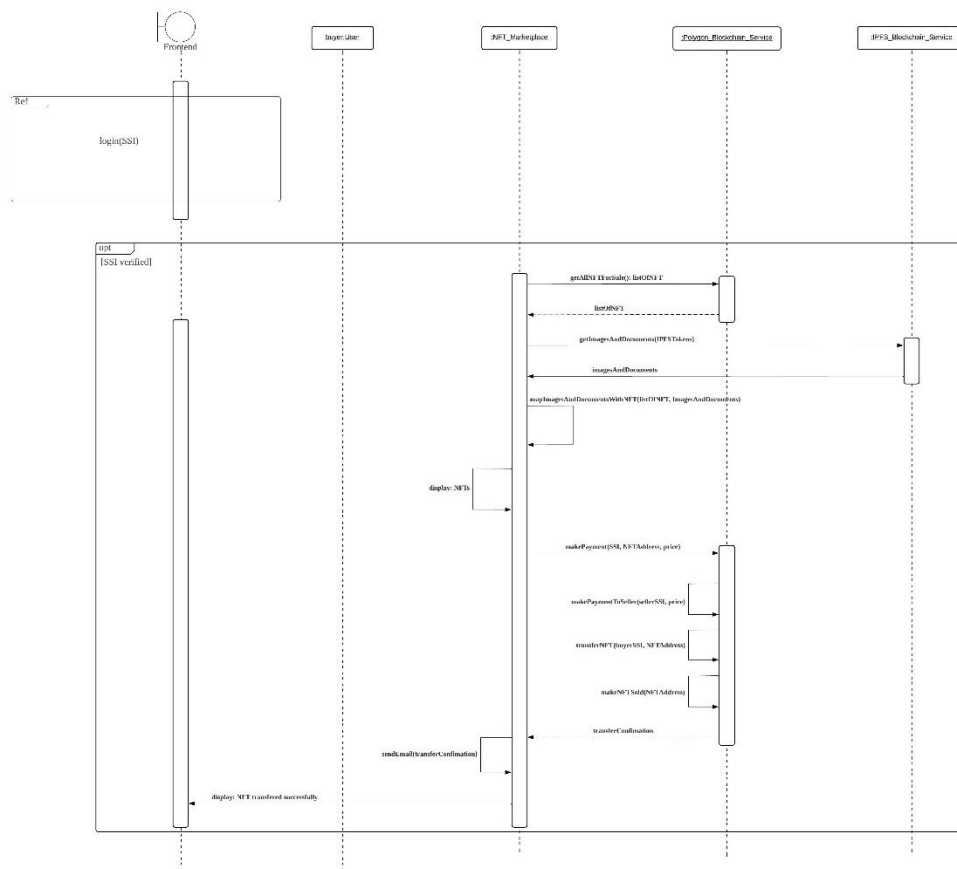


Figure 5-15 Sequence Diagram NFT Market Place (to buy a vehicle)

5.3.5 ER Diagram

Note: Our main reason to use a database is not to save our permanent data on those databases. For that purpose, we use blockchains. But we need a database to maintain the usability and email verification of the system. We want to save those data until do a proper email verification to avoid spam emails. Therefore, there is no need to save these data in the blockchain. It is a high-cost work. That is the only requirement to use a database in this system. Please find below the ER diagram corresponding to the database.

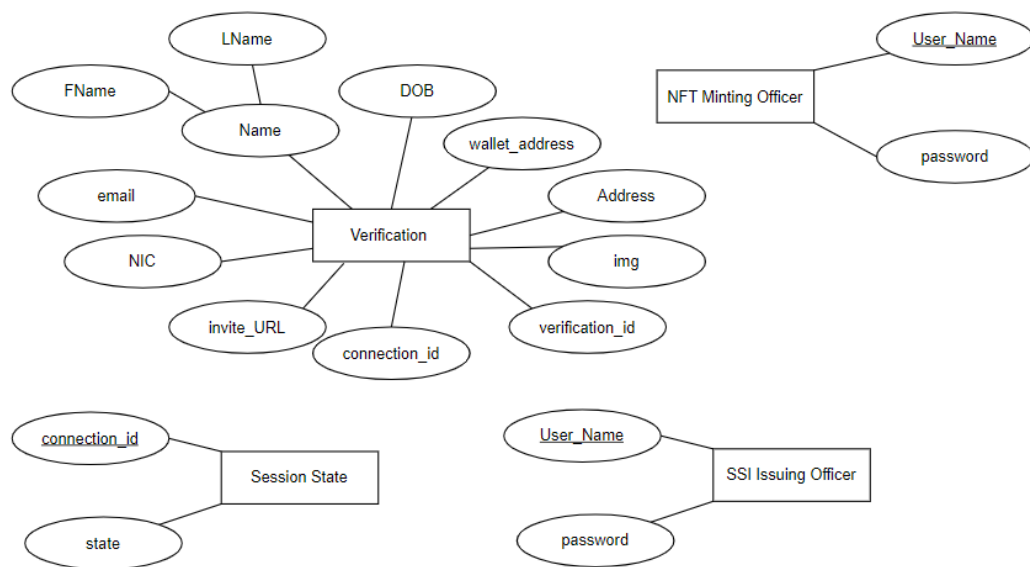


Figure 5-17 ER Diagram

5.4 Summary

Through this chapter analysis and design, the diagrams like Use case, Class, Activity and Sequence were presented and they provide the basic understanding about design and analysis of the project. The next chapter provides the strategies followed for implementing modules.

Chapter 6 Implementation

6.1 Introduction

In chapter 5, we outlined how we gathered the requirements of the client and started to design the system after identifying the issue. This chapter provides the strategies followed for implementing modules. In the implementing process the application is divided into five parts like SSI Issuer, SSI Verifier, Mobile SSI wallet, NFT Minter, and NFT Marketplace. We selected the waterfall model as our software process model. Currently we are developing the frontend and the backend of the system. And also, we have finished a huge proportion of the backend developing and it stays in a stable state. Moreover, we are hoping to develop the interfaces of the system.

6.2 SSI Issuer

In our project Blockchain Based Vehicle Registration and Ownership Management System, we are using SSI- Self Sovereign Identity which is an ID to identify the vehicle owner which is a digitally verifiable ID. We can use this ID to log in and log out of the digital NFT marketplace (vehicle). The data for the SSI creation form comes from the general user and that data is provided via a form filled by the general user manually. This is a closed system that can be only accessed by the SSI issuing person. When we considering about the implementation, basic system of issuing application is implementing. The authentication and authorization part has not be completed.

6.3 SSI Verifier

The SSI verifier verifies the SSI which is sent by the NFT minter, NFT marketplace and other necessary parties. It is verified by using the Indy blockchain and sending a message as response confirming the validation of the details. The basic system for the SSI Verifier has not been completed. Because the authentication and authorization are not completed yet in this part.

6.4 Mobile SSI Wallet

The SSI (Self-sovereign identity) which is issued for users through the SSI issuer system. This mobile application is used by normal citizens and especially our target audience is the ones who use the vehicle marketplace. When any third-party person needs to check the identity of any person, that third-party person can check that person's SSI (which is stored in this mobile application) and identify that person. Up to now

proof of concept has been implemented for this part of the project. Wireframes related to the mobile application have been completed.

6.5 NFT Minter

In our system, after issuing a Self-Sovereign Identity (SSI), we want to register their vehicle also. We used a Nonfungible Token (NFT) to represent the vehicle in our marketplace. To do that, we mint an NFT with all details of the vehicle and transfer ownership. This is a closed system. This system is used by only authorized persons in a particular company. When a vehicle is registered for the first time the vehicle owner wants to go to that company to register his vehicle with all necessary details. Up to now proof of concept (POC) has been implemented for this part of the project.

6.6 NFT marketplace

In our system, we have a platform to sell and buy vehicles. This is an open system for any user. Anyone can access the system through their Self Sovereign Identity (SSI). Up to now proof of concept (POC) has been implemented for this part of the project.

6.7 Triggers and Implementation

Images of the implemented parts is in the appendix B.

6.8 Version Controlling

We use GitHub as our version controlling platform.

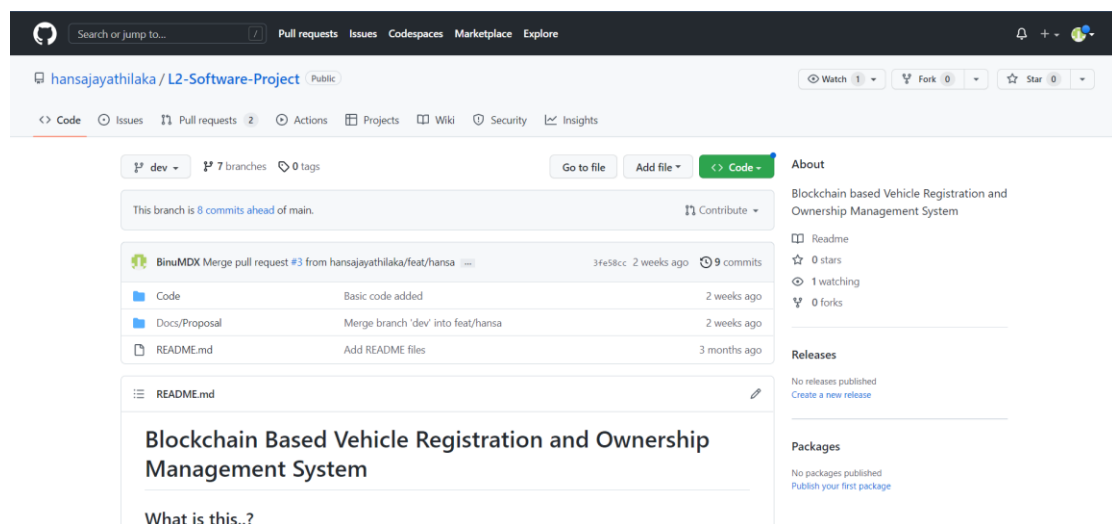


Figure 6-1 Version Controlling GitHub platform

6.9 Summary

In this chapter we have already outlined the strategies that we have followed for implementing modules. Our application has divided into five parts like SSI Issuer, SSI Verifier, Mobile SSI wallet, NFT Minter, and NFT Marketplace. In the next chapter we will discuss the evaluation and testing of our solution and how our solution differs from other solutions in the market, further developments, and implementation.

Chapter 7 Discussion

7.1 Introduction

In the previous chapter, we discussed the implementation of our system up to now. Through this chapter, we discuss the evaluation and testing of our solution and how our solution differs from other solutions in the market, further developments, and implementation is also discussed in this chapter.

7.2 Evaluation and Testing

Currently, we have not evaluated or tested our solution as we are currently in the initial stage of development. So, through this chapter we like to discuss how our solution differs from other products in the market.

7.3 How Our Solution Differs from Other Solutions

The projects that we have discussed in chapter 2 were implemented slightly similarly to our blockchain-based vehicle registration and ownership management system. Therefore, there are some differences between similar projects and our project. In section 2.2 they created a very similar project to our system although it remains a mere idea at this moment. But in that project, they just save their data in the blockchain rather than minting an NFT. There is no standard in their project, and it is just a custom smart contract. But we are going to implement ERC 721 Standard NFT. The specialty of this standard is that we can sell these NFTs in any NFT marketplace. The difference between the section 2.3 Sandbox project with ours is that they are selling and buying virtual assets (land) instead of real assets. But in our project, we are dealing with real physical assets (vehicles). And also, when taking section 2.4 OpenSea project, its trade in intangible, digital goods, our project deals in tangible, physical assets - specifically, vehicles. So that our project is different from what we researched previously. And it is more complex and secure than all those mentioned projects. That is why our project is worthier than the existing projects.

7.4 Further Development

As further development we expect to introduce a new cryptocurrency to do transactions in the marketplace when selling and buying vehicles. And also, we are expecting to add a verification with the database maintained by the government with vehicle details parallel to the manual verification process.

7.5 Summary

In this chapter, mainly the evaluation and the testing of our project were discussed. The other solutions similar to our project and how they differ from our solution and each other were described here. As well as new additions for our project were mentioned under the further development.

Chapter 8 References

- [1] S. M. H. Bamakan, N. Nezhadsistani, O. Bodaghi, and Q. Qu, “Patents and intellectual property assets as non-fungible tokens; key technologies and challenges,” *Sci Rep*, vol. 12, no. 1, Dec. 2022, doi: 10.1038/s41598-022-05920-6.
- [2] “Difference between Centralized Database and Distributed Database - GeeksforGeeks.” <https://www.geeksforgeeks.org/difference-between-centralized-database-and-distributed-database/> (accessed Dec. 24, 2022).
- [3] “What is Blockchain Technology? - IBM Blockchain | IBM.” <https://www.ibm.com/topics/what-is-blockchain> (accessed Dec. 24, 2022).
- [4] “Blockchain vs Database: Understanding The Difference.” <https://101blockchains.com/blockchain-vs-database-the-difference/> (accessed Dec. 24, 2022).
- [5] “Non-Fungible Tokens (NFTs) Explained | AWS Blockchain.” <https://aws.amazon.com/blockchain/nfts-explained/> (accessed Dec. 24, 2022).
- [6] “Mutability - Definition, Meaning & Synonyms | Vocabulary.com.” <https://www.vocabulary.com/dictionary/mutability> (accessed Dec. 24, 2022).
- [7] Institute of Electrical and Electronics Engineers. Bangladesh Section, IEEE Region 10, and Institute of Electrical and Electronics Engineers, *2020 IEEE Region 10 Symposium (TENSYP) : 5-7 June 2020, Dhaka, Bangladesh*.
- [8] M. Dowling, “Fertile LAND: Pricing non-fungible tokens,” *Financ Res Lett*, vol. 44, p. 102096, Jan. 2022, doi: 10.1016/J.FRL.2021.102096.
- [9] V. Nakavachara and K. Saengchote, “Does unit of account affect willingness to pay? Evidence from metaverse LAND transactions,” *Financ Res Lett*, vol. 49, p. 103089, Oct. 2022, doi: 10.1016/J.FRL.2022.103089.
- [10] “OpenSea: Diving into the World of NFTs — AMT Lab @ CMU.” <https://amt-lab.org/reviews/2022/1/opensea-diving-into-the-world-of-nfts> (accessed Dec. 23, 2022).
- [11] “Top 16 NFT Marketplaces for Creators to Sell Non-Fungible Tokens in 2023.” <https://influencermarketinghub.com/nft-marketplace/#toc-0> (accessed Dec. 24, 2022).

- [12] “OpenSea: Diving into the World of NFTs — AMT Lab @ CMU.” <https://amt-lab.org/reviews/2022/1/opensea-diving-into-the-world-of-nfts> (accessed Dec. 24, 2022).
- [13] “What is Web 2.0 - Definition, Advantages and Features.” <https://www.znetlive.com/blog/web-2-0/> (accessed Dec. 25, 2022).
- [14] “ReactJS - Introduction.” https://www.tutorialspoint.com/reactjs/reactjs_introduction.htm (accessed Dec. 25, 2022).
- [15] A. Carcangiu, G. Fenu, and L. D. Spano, “A design pattern for multimodal and multidevice user interfaces,” in *EICS 2016 - 8th ACM SIGCHI Symposium on Engineering Interactive Computing Systems*, Jun. 2016, pp. 177–182. doi: 10.1145/2933242.2935876.
- [16] “React Native · Learn once, write anywhere.” <https://reactnative.dev/> (accessed Dec. 25, 2022).
- [17] “What is Next.js? - Enonic.” <https://enonic.com/blog/what-is-next-js> (accessed Dec. 25, 2022).
- [18] H. Gore *et al.*, “Django: Web Development Simple & Fast,” 2021. [Online]. Available: <http://annalsofrscb.ro>
- [19] “PostgreSQL: The world’s most advanced open source database.” <https://www.postgresql.org/> (accessed Jan. 01, 2023).
- [20] “What is Web 3.0? - Definition from TechTarget.com.” <https://www.techtarget.com/whatis/definition/Web-30> (accessed Dec. 25, 2022).
- [21] “What is Blockchain Technology? - IBM Blockchain | IBM.” <https://www.ibm.com/topics/what-is-blockchain> (accessed Dec. 25, 2022).
- [22] “AWS Marketplace: Hyperledger Indy (HVM).” <https://aws.amazon.com/marketplace/pp/prodview-2ogkmzoksqkru> (accessed Dec. 25, 2022).
- [23] “Polygon blockchain explained: A beginner’s guide to MATIC.” <https://cointelegraph.com/blockchain-for-beginners/polygon-blockchain-explained-a-beginners-guide-to-matic> (accessed Dec. 25, 2022).
- [24] “What Is IPFS?” <https://beincrypto.com/learn/what-is-ipfs/> (accessed Dec. 25, 2022).

- [25] “aries-cloudagent-python/DevReadMe.md at main · hyperledger/aries-cloudagent-python.” <https://github.com/hyperledger/aries-cloudagent-python/blob/main/DevReadMe.md> (accessed Dec. 25, 2022).
- [26] “MetaMask Wallet Review 2022.” <https://www.investopedia.com/metamask-cryptocurrency-wallet-review-5235562> (accessed Dec. 25, 2022).
- [27] “What is Docker? | IBM.” <https://www.ibm.com/topics/docker> (accessed Dec. 26, 2022).
- [28] “Overview | Docker Documentation.” <https://docs.docker.com/compose/> (accessed Dec. 26, 2022).

Appendix A - Individual Contribution

204047J Dissanayake DMBM – NFT Minter

As the leader of the team my responsibilities are to arrange meetings with mentors, supervisors, manage the project, arrange knowledge sharing sessions, manage the git repository and to share tasks among other team members correctly. As a team member I was assigned to do the NFT Minter module.

I could successfully arrange meetings with our supervisor in which we gained knowledge and resolved errors and mistakes. Moreover, I arranged knowledge sharing sessions and as a result every member will be able to implement a module fully functional with frontend and backend. While doing the project I and another member managed a git repository for our project and every member uploaded their module to the repository. Furthermore, I used Jira project management tool to manage the project. I contributed to the designing phase by drawing diagrams.

In the NFT minter module, Blockchain–Based Vehicle Registration and Ownership Management System, after issuing a Self-Sovereign Identity (SSI), we want to register their vehicle also. We used a Nonfungible Token (NFT) to represent the vehicle in our marketplace. To do that, we mint an NFT with all details of the vehicle and transfer ownership. This is a closed system. This system is used by only authorized persons in a particular company. When a vehicle is registered at first time the vehicle owner wants to go to that company to register his vehicle with all necessary details.

I am learning ReactJs as frontend technology, smart contract and ERC-721 tokens.

204074M Herath PAUD - Mobile SSI wallet

I was assigned to develop the Mobile SSI wallet module. I contributed to the designing phase by drawing use case diagram, class diagram, sequence diagram, activity diagram and ER diagram.

The SSI (Self-Sovereign Identity) which is issued for users through the SSI issuer system. This mobile application is used by normal citizens and especially our target audience is the ones who use the NFT marketplace. When any third-party person needs to check the identity of any person that third-party person can check that person's SSI (which is stored in this mobile application) and identify that person.

In the SSI Mobile Wallet module, after entering the password then the general user can login to the Mobile SSI Wallet. Then the home page of the wallet will be displayed. To make a connection with a SSI Issuer first have to scan the QR Code issued by the SSI Issuer. After the connection is established, the SSI issuer will send the relevant SSI to this mobile wallet through connection and that sent credential will be saved.

204087F Jayathilaka PHP -NFT Marketplace

I was assigned to develop the NFT marketplace. I contributed to the designing phase by drawing use case diagram, class diagram, sequence diagram, activity diagram and ER diagram.

In our Blockchain – Based Vehicle Registration and Ownership Management System, we have a platform to sell and buy vehicles. This is an open system for any user. Anyone can access the system through their Self Sovereign Identity (SSI).

In the NFT marketplace module, upon logging in with their SSI credentials, the general user is able to view a selection of vehicles available for sale on the home page of NFT Marketplace. In the home page there can be seen each vehicle as a card with an image of that vehicle and few details. After clicking on any card, the general user is directed to a page which can be seen all the details (past owners, price, vehicle technical details, vehicle number, etc.) related to that vehicle. There is a separate tab to view the NFTs which belong to that user. There is a separate button to move to the selling pages. And the seller can fill in a few data fields and make a particular NFT available for selling. And if any buyer needs to buy a particular vehicle, that person can click on the vehicle card that he wants to buy. And after clicking there is an option to buy that vehicle and after using that option the buyer can do the transaction using cryptocurrency. And then the transaction happens with the aid of the MetaMask wallet and the ownership of the NFT is transferred to the new owner. Also, while doing the project, I and other member managed a git repository for our project and every member uploaded their module to the repository.

204150T Pathirana SPSN -SSI Verifier

I was assigned to develop the Mobile SSI verifier module in Blockchain – Based Vehicle Registration and Ownership Management System. I contributed to the designing phase by drawing use case diagram, class diagram, sequence diagram, activity diagram and ER diagram.

The SSI verifier verifies the SSI which is sent by the NFT minter, NFT marketplace and other necessary parties. It is verified by using the Indy blockchain and sending a message as response confirming the validation of the details. There are two verifying processes related to our project. One is SSI verifier module will be used in the login to the NFT Marketplace. The other verifying approach is that the third-party person (such as police officers) can use this SSI Verifier to check whether the real identity of a general person. This module is beneficial to find the real identity of a person in day-to-day life normal activities.

In the SSI verifier module, there is a QR code to scan to the users. In addition to, there are three features like link to open in a trusted wallet, invitation link and copy invitation link.

I started to learn Django framework for backend technology.

204179N Rathnayaka AMDB -SSI Issuer

In our project Blockchain Based Vehicle Registration and Ownership Management System I was assigned to develop the SSI Issuer module. I contributed to the designing phase by drawing use case diagram, class diagram, sequence diagram, activity diagram, ER diagram.

In the Blockchain Based Vehicle Registration and Ownership Management System, we are using SSI- Self Sovereign Identity which is an ID to identify the vehicle owner which is a digitally verifiable ID. We can use this ID to log in and log out of the digital NFT marketplace (vehicle). The data for the SSI creation form comes from the general user and that data is provided via a form filled by the general user manually. This is a closed system that can be only accessed by the SSI Issuing person.

In the SSI Issuer module, first the SSI issuing officer submits the already provided username and the password then he or she can log in to the system. After login he or she directs into a SSI generating details form. Then that form will be filled out by the SSI issuing officer and provided as input for the system. As a result of that form submission, the SSI Issuer module will generate a SSI. Then a verifiable email will be sent to the relevant email address which is provided in the SSI requesting form. In that email, there is a link to verify the email provided. After verifying the email, a QR code and a link will be displayed. After scanning the QR code using the SSI Mobile Wallet or clicking the link the general user can make a connection through the system with the SSI Mobile Wallet. According to the generated connection with the SSI Mobile Wallet, this SSI Issuer module will send the SSI which is generated related to the submitted data of that general user.

I am learning Django 3 framework for backend technology.

Appendix B

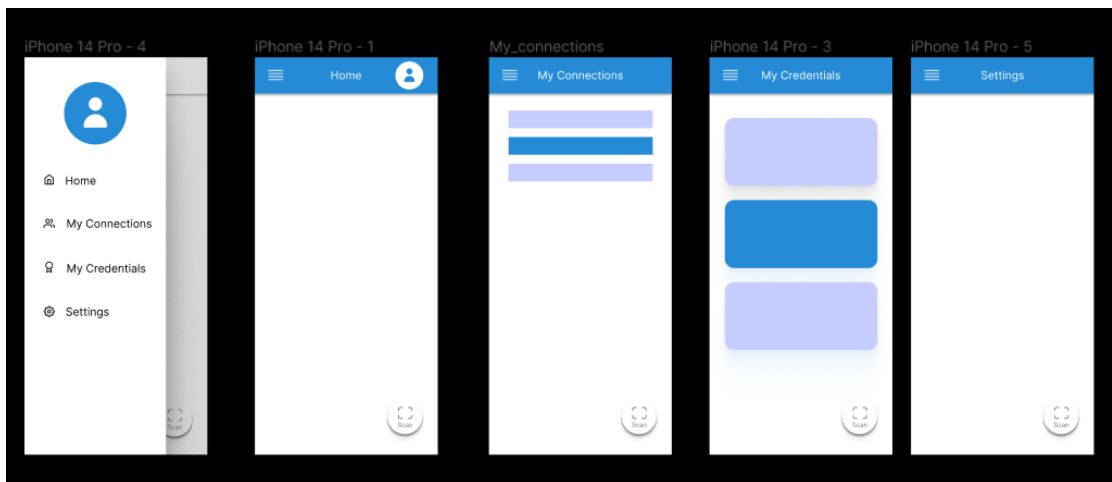


Figure 8-1 Mockup Mobile SSI Wallet

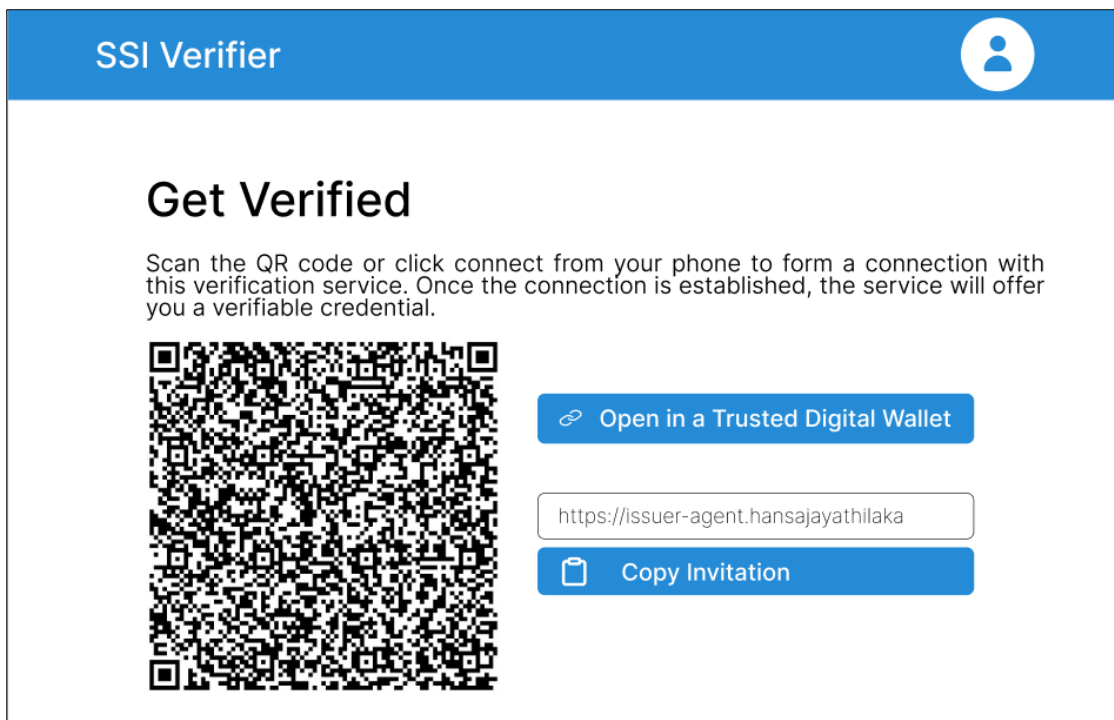


Figure 8-2 Example of Generated QR code

SSI Requesting Form

Full Name

Full Name

NIC Number

NIC Number

Email

Email

Date of Birth

Year

Month

Day

Telephone Number

Telephone Number

Permanent Address

Country

District

State

City

Postal Code

Current Address

Country

District

State

City

Postal Code

Occupation

Occupation

Gender

☐ Male
 ☐ Female
 ☐ Other

Civil Status

Single

Crypto Wallet Address

Crypto Wallet Address

Submit

Figure 8-3 Mockup of SSI Issuing Application

NFT Requesting Form

Vehicle Details

Current Owner

Eg: ABC Perera, No 15, Colombo 14

Absolute Owner

Eg: ABC Perera, No 15, Colombo 14

Engine No

Eg:5FGHJ5265

Class of Vehicle

Eg: Car

Status when Registered

Eg: Brand New

Make

Eg: Toyota

Model

Eg: Premio

Wheel Base

Eg: 145 cm

Type of Body

Eg: Platform

Colour

Eg: White

Seating Capacity

Eg: four

Internal Height

Internal Height

Date of First Registration

Date of First Registration

Cylinder Capacity

Cylinder Capacity

Previous Owner

Eg: ABC Perera, No 15, Colombo 14

Fuel Type

Eg: Diesel

Submit

Figure 8-4 Mockup of UI NFT Minting Application

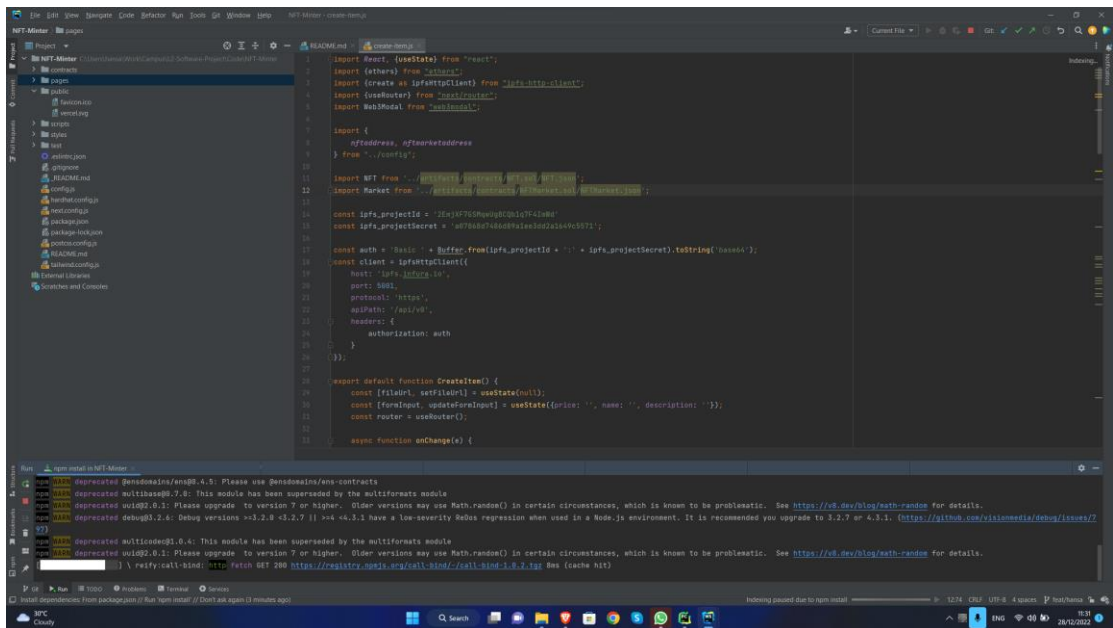


Figure 8-5 Implementation Backend 204047J

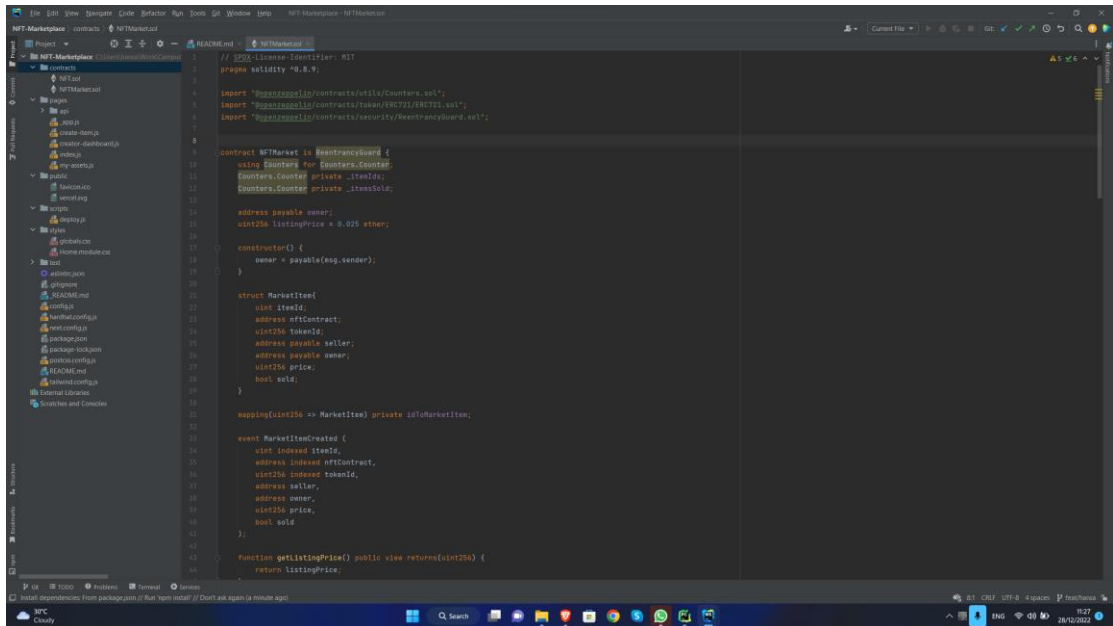


Figure 8-6 Implementation Backend 204087F

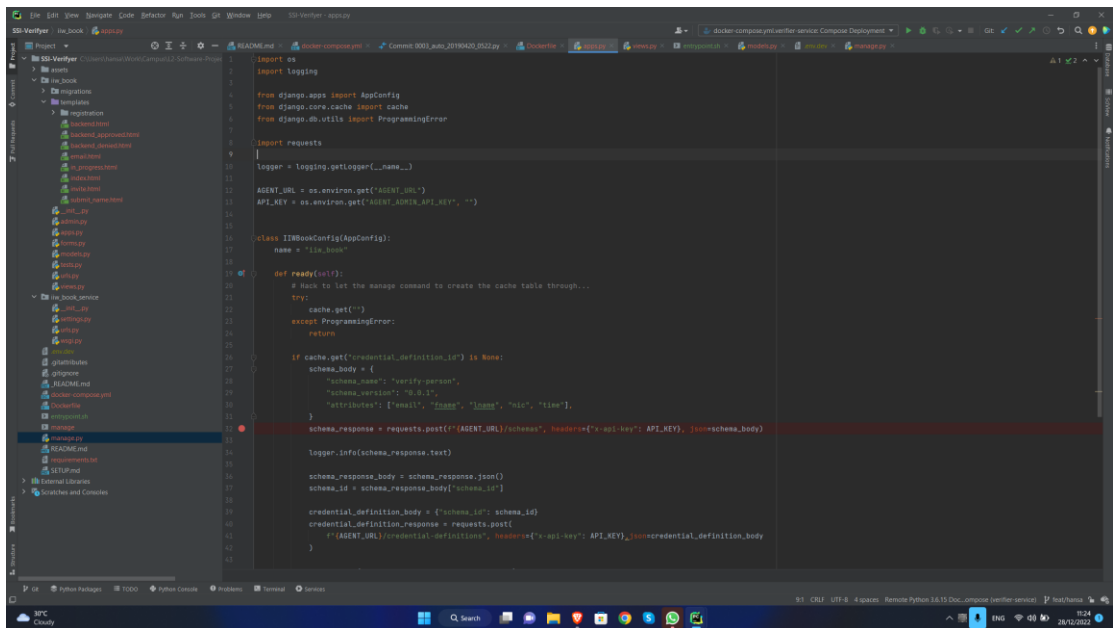


Figure 8-7 Implementation Backend 204150T

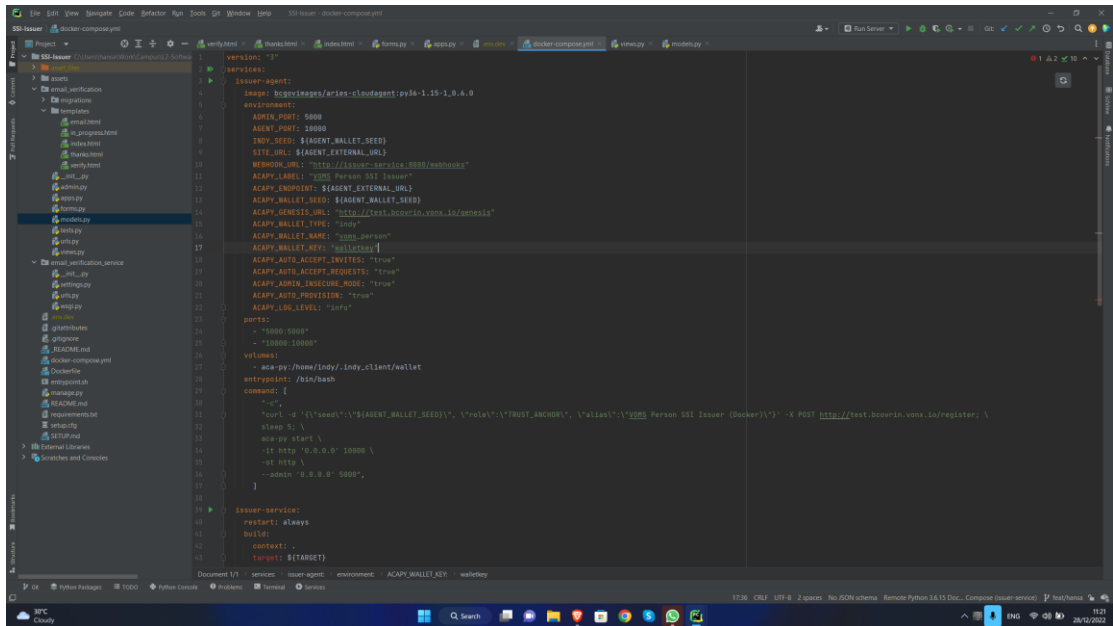


Figure 8-8 Implementation Backend 204179N

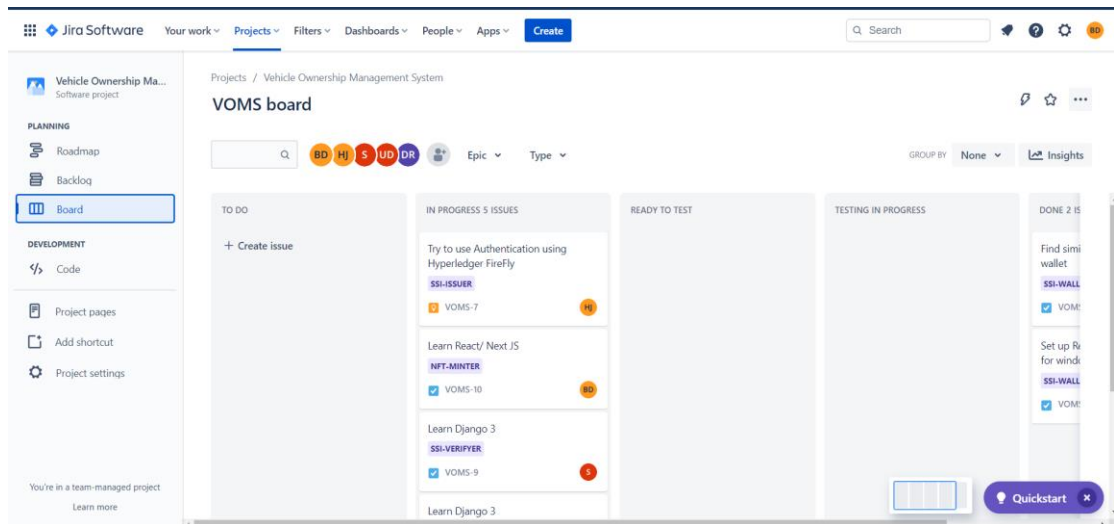


Figure 8-9 Jira as Project Management tool

Appendix C – Plan of Action

| | 2022 | | | | 2023 | | | | | | | |
|---------------------------------------|------|-----|-----|-----|------|-----|-----|-----|-----|-----|------|-----|
| | Sep | Oct | Nov | Dec | Jan | Feb | Mar | Apr | May | Jun | July | Aug |
| Study about blockchain, React, Django | | | | | | | | | | | | |
| Requirements gathering and analysis | | | | | | | | | | | | |
| System Develop | | | | | | | | | | | | |
| Implement web application | | | | | | | | | | | | |
| Implement mobile application | | | | | | | | | | | | |
| System Testing | | | | | | | | | | | | |
| Finalize the project | | | | | | | | | | | | |

Appendix D – User Stories

- As a general user, I want to give my data to the SSI issuing officer via a hard copy, so that I can request an SSI.
- As a general user, I want a SSI, so that I can log into the NFT marketplace.
- As a SSI issuing officer, I want login credentials, so that system will prevent unauthorized access.
- As a SSI issuing officer, I want to validate data, so that the system can avoid misuse of SSI.
- As a general user, I want to verify email, so that I will prevent from entering invalid email.
- As a vehicle owner, I want an NFT, so that I can sell my vehicle in the NFT marketplace.
- As an NFT minting officer, I want login credentials, so that system will prevent unauthorized access.
- As a buyer, I want to select an NFT, so that I can buy a vehicle.

Software Requirements Specification

for

Vehicle Registration and Ownership Management System

Prepared by Troyrangers

Faculty of Information Technology

University of Moratuwa

24/12/2022

Table of Contents

| | |
|-----------------------------------------------------|-----------|
| Table of Contents | ii |
| Revision History | ii |
| 1. Introduction..... | 1 |
| 1.1 Purpose..... | 1 |
| 1.2 Document Conventions..... | 1 |
| 1.3 Intended Audience and Reading Suggestions | 1 |
| 1.4 Product Scope | 1 |
| 1.5 References..... | 2 |
| 2. Overall Description..... | 3 |
| 2.1 Product Perspective..... | 3 |
| 2.2 Product Functions | 3 |
| 2.3 User Classes and Characteristic | 3 |
| 2.4 Operating Environment..... | 4 |
| 2.5 Design and Implementation Constraints | 4 |
| 2.6 User Documentation | 4 |
| 2.7 Assumptions and Dependencies..... | 4 |
| 3. External Interface Requirements | 5 |
| 3.1 User Interfaces | 5 |
| 3.2 Hardware Interfaces | 5 |
| 3.3 Software Interfaces | 6 |
| 3.4 Communications Interfaces..... | 6 |
| 4. System Features | 7 |
| 4.1 SSI Issuing Process | 7 |
| 4.2 SSI Verifying Process | 8 |
| 4.3 NFT Minting Process..... | 9 |
| 4.4 Mobile SSI Wallet..... | 10 |
| 4.5 NFT Market Place..... | 11 |
| 5. Other Nonfunctional Requirements..... | 13 |
| 5.1 Performance Requirements | 13 |
| 5.2 Safety Requirements | 13 |
| 5.3 Security Requirements | 13 |
| 5.4 Software Quality Attributes | 13 |
| 5.5 Business Rules | 14 |
| 6. Other Requirements | 15 |
| Appendix A: Glossary..... | 16 |
| Appendix B: Analysis Models | 17 |

Revision History

| Name | Date | Reason For Changes | Version |
|------|------|--------------------|---------|
| | | | |
| | | | |

1. Introduction

1.1 Purpose

The main purpose of this document is to describe and to demonstrate the functionality of the Vehicle Ownership Management system. It contains a detailed description of all the functional and non-functional requirements of the system. Also, this document shows the purpose and complete declaration of the system and explains system constraints and interactions with system users.

1.2 Document Conventions

IEEE 830-1998 standard for writing SRS documents was used in preparing this SRS document.

1.3 Intended Audience and Reading Suggestions

This document will be helpful to project managers, developers, users and testers of the system to get an idea about the functionalities of this system. We recommend project managers and users to go through the overall description of this document. Developers and testers are recommended to read the functional and non-functional requirements and the external interface requirements of this document.

1.4 Product Scope

Vehicle Registration and Ownership Management System is an application which is used to digitize the registration and ownership management system of vehicles. We implement our system with security and transparency, as security is the most required factor in these kinds of systems. Therefore, it is not much better to use a centralized database, and therefore as the best way, we use a blockchain. The main task of our system is to convert a physical asset into a digital asset. As an example, in our system we convert vehicle asset into a NFT (Non-Fungible Token).

There is a special process that happened in registering the vehicle. When we are registering the vehicle, we can mint (create) NFT with all details of the vehicle. According to that, there can be photographs of the vehicle according to the standards,

and also all the information related to the vehicle which are included in the scanned copy of vehicle registration book. Not only that, but also, we create a vehicle marketplace to provide the facility of selling and buying vehicles. In this process, transferring the ownership of the vehicle happens through the NFT. When the lifetime of the vehicle is over, we have to remove the vehicle of use. In that case we can burn-out related NFT. But the information related to that NFT will remain forever with that blockchain. In the current situation, we have to identify a person legally on the internet. But there is not a proper way to show a person's digital identity. That means a person can't be legally identified in internet. Because of that we have to issue a digital verifiable ID for them. As we can identify the vehicle owner through this digital verifiable ID, we can use this ID to login the digital marketplace.

1.5 References

IEEE 830-1998 standard for writing SRS document.

2. Overall Description

2.1 Product Perspective

This system is newly introduced software. But it is a replacement for the current NIC issuing system and existing vehicle ownership registration system. The blockchain based vehicle registration and ownership management system is a web-based application which contains a mobile application that can be used to register a vehicle as a NFT and, record all the details of the vehicle and it also has a market environment that can buy and sell those registered vehicles and legally transfer ownership within the system. And this application contains the ability of register a person and verify this person by giving an SSI.

2.2 Product Functions

1. User shall be able to request a SSI
2. User shall be able to request a NFT for his/ her vehicle.
3. User shall be able to store their SSI.
4. User shall be able to buy a vehicle through the NFT
5. User shall be able to sell a vehicle through the NFT

2.3 User Classes and Characteristic

Users of this application are General user, SSI issuing officer, Seller, Buyer, Vehicle owner, and NFT minting officer.

General users give a hard copy of SSI request form to SSI issuing officer. The SSI issuing officer logs into the system and enters user's details into the system which is included in the SSI requesting form.

The vehicle owner can sell a vehicle through the marketplace and he or she wants to get a NFT which represents their vehicle. NFT minting officer enters vehicle's details into the system which is included in the NFT request form. If user is a seller and he or she wants to open a request to sell his vehicle, then the NFT of this vehicle is marked as sale. If the user is a buyer, then he can see all NFTs which are in the selling state with the price.

2.4 Operating Environment

Since our project is a web application it will follow the standard client server model. The UI of our application is compatible with Desktop, Laptop and Mobile Device screens. Data will be stored on a cloud-based system using Amazon Web Services as the cloud provider.

2.5 Design and Implementation Constraints

- Front end of the application will be designed using ReactJs + NextJS, Html and CSS, React Native
- We will use Django to design the backend.
- Blockchain technology is used to save our data.

2.6 User Documentation

We include online help in the application.

2.7 Assumptions and Dependencies

The SSI issuing application and NFT minting application should be included in an internal network. Public users can't access them. All the users of the system should be connected to the internet for proper functioning of the system.

3. External Interface Requirements

3.1 User Interfaces

3.1.1 SSI Issuing Application

There is a one GUI for the login of the issuing officer. And also, there is another user interface for the SSI request form.

3.1.2 SSI Verifying Application

There is a third-party verification GUI and verification API.

3.1.3 Mobile SSI Wallet

There is a mobile application UI. This stores SSI, present SSI. And also, scans the QR, and manages the SSI.

3.1.4 NFT minter

There is a one GUI for the login of NFT minting officer. And there is another user interface for the NFT request form.

3.1.5 Marketplace

There are GUIs for the login of seller/ buyer, marketplace operations such as listing NFTs, get NFT full details, updating NFT description, buy, sell.

3.2 Hardware Interfaces

In this system we expect to implement as a web-based application and a mobile application system. So, any device can work with any kind of web browser, this system can also access without any interruption.

This system does not need specific internet speed or extra CPU or GPU power, there normal data processing exists. So that a device depends on some particular hardware specification for normal browsing, it will be the minimum hardware requirement for running this application.

3.3 Software Interfaces

3.3.1 Indy

Our system communicates with the Indy blockchain using Aries cloud agent python software interface.

3.3.2 Polygon

Hardhat, Web3model, ethers are three JavaScript libraries. Communication between the system and the polygon blockchain happens through these libraries.

3.3.3 IPFS

“ipfs- http-client” is a java script library. All the communications of the system are happened through this library.

3.4 Communications Interfaces

- In this system, the API is needed to communicate between Django and Aries Cloud Agent python (ACA-Py).
- We implement an Email service in the Communication interface.
- Application and backend communication will happen on HTTPS web requests.
- There are two web servers for SSI issuer and SSI verifier.
- We make an SSL certificate chain, and there is a self-sign certificate`` in between the server and cloud flare.

4. System Features

This illustrates organizing the functional requirements for the product by system features, the major services provided by the product. We can divide the functional requirements into the following categories.

4.1 SSI Issuing Process

4.1.1 Description and Priority

For a person he or she must have a unique identity which is digitally verifiable to log in to the blockchain based vehicle registration management system. Therefore, each person has to generate his own SSI. That part is done by using this SSI Issuer system. This part has the highest priority. Without the SSI for a particular person, he or she can't log in to the system. And the penalty of not creating this SSI Issuer module is that we can't mint a NFT without a SSI and this SSI generating part will be done by using this SSI Issuer module. Cost can be represented according to three ways as time, money, and labor. To develop this module, one developer has to work for nearly 5 months. As the monetary cost of this module, we have to spend for servers to host the private blockchain. The risk to develop this SSI Issuer part is that this uses blockchain technology and it is quite new and an evolving technology. And therefore, it is hard to find resources to develop this particular module.

4.1.2 Stimulus/Response Sequences

First the SSI issuing officer submits the already provided username and the password then he or she can log in to the system. After login he or she directs into a SSI generating details form. Then that form will be filled out by the SSI issuing officer and provided as input for the system. As a result of that form submission, the SSI Issuer module will generate a SSI. Then a verifiable email will be sent to the relevant email address which is provided in the SSI requesting form. In that email, there is a link to verify the email provided. After verifying the email, a QR code and a link will be displayed. After scanning the QR code using the SSI Mobile Wallet or clicking the link the general user can make a

connection through the system with the SSI Mobile Wallet. According to the generated connection with the SSI Mobile Wallet, this SSI Issuer module will send the SSI which is generated related to the submitted data of that general user.

4.1.3 Functional Requirements

REQ-1: The system should display a login page for the SSI issuing officer

REQ-2: The system should allow entering a SSI requesting form.

REQ-3: The system should generate a SSI related to the submitted data.

REQ-4: The system should allow making a connection with the SSI Mobile wallet.

REQ-5: The system should send a verifiable email to the general user.

4.2 SSI Verifying Process

4.2.1 Description and Priority

The SSI Verifier offers two unique approaches for verifying your identity. The first and the most important verifying process related to our project is that this SSI verifier module will be used in the login to the NFT Market Place. The other verifying approach is that the third-party person (such as police officers) can use this SSI Verifier to check whether the real identity of a general person. This module has a higher priority. Because without this module we can't filter the ones who are eligible to enter the NFT Market Place. And other than that, this module is beneficial to find the real identity of a person in day-to-day life normal activities. If we do not develop this module the penalty is that we won't be able to filter the users for the NFT Market Place. Cost can be represented according to three ways as time, money, and labor. To develop this module, one developer has to work for nearly 5 months. When taking the monetary cost for this module, the SSI Verifier module will be built on top of Hyperledger Indy, and for this, we have to use a private blockchain, therefore the monetary cost is only for the servers.

4.2.2 Stimulus/Response Sequences

There are two distinct stimulus interactions that happen with SSI Verifier module. When taking the first interaction process, that SSI verifier has a QR code and that is read using the SSI Mobile Wallet. Then the SSI will be sent to the SSI Verifier. And as a result of that, if the SSI is valid then the user will be directed to the NFT Market Place Home page and if it is not then the user will be provided with an error message.

4.2.3 Functional Requirements

REQ-6: The system must verify the Self-Sovereign Identity (SSI).

4.3 NFT Minting Process

4.3.1 Description and Priority

When a vehicle owner wants to sell a vehicle through the NFT marketplace, he or she wants to generate an NFT which represents their vehicle. The NFT is minted in the polygon blockchain with the help of the NFT minting officer (because this person is the one who is responsible to submit the data related to the vehicle). And then the ownership of the NFT is transferred to the owner of the vehicle. Without an NFT, the vehicle owner can't sell a vehicle within the system.

The benefit of this NFT Minting module is that we can digitize and give a digital identity to a real-world existing vehicle. And that will help to maintain an easily manageable (because we do not have a hard legal background to change the ownership of a vehicle and we can just simply record the transaction on the Polygon blockchain) and secure NFT Vehicle Marketplace. For this NFT Minter, we use Polygon Blockchain which is a public blockchain. Therefore, we have to bear a cost for each transaction in a public blockchain.

4.3.2 Stimulus/Response Sequences

NFT Minting Officer submits the data relevant to a vehicle which is provided by a vehicle owner to the NFT Minter module. As a result of that the NFT minter module will generate a NFT related to that provided data. After the creation of the NFT that NFT can be seen in the NFT Marketplace.

4.3.3 Functional Requirements

REQ-7: The system must provide a facility for the NFT minting officer to log in to the system.

REQ-8: The system must display a form to enter the details of vehicle.

REQ-9: The system must create the NFT based on the provided data.

REQ-10: The system must change the ownership of the NFT when selling and buying vehicles.

4.4 Mobile SSI Wallet

4.4.1 Description and Priority

The general user can buy or sell a vehicle within the NFT Marketplace and to involve that process that particular person must have a SSI to log in to that Marketplace. For that, the user should scan a QR code from his or her mobile SSI wallet and after scanning that QR code, the mobile SSI wallet establishes a connection between the SSI Verifier and that SSI Mobile Wallet. After that connection was established that SSI will be sent to the SSI verifier module. This is the benefit of this module. If this module won't developed, then there is not a way to store the SSI which is used to identify a general user. For this Mobile SSI Wallet, we use Hyperledger Indy which is a private blockchain. Therefore, we have to bear a cost only for servers.

4.4.2 Stimulus/Response Sequences

After entering the password then the general user can login to the Mobile SSI Wallet. Then the home page of the wallet will be displayed. To make a connection with a SSI issuer first have to scan the QR Code issued by the SSI Issuer. After the connection is established SSI issuer will send the relevant SSI to this mobile wallet and that sent credential will be saved.

4.4.3 Functional Requirements

REQ-11: The system must provide a facility to scan the QR code.

REQ-12: The system must store and display the credentials.

REQ-13: The system must store and display the connections.

4.5 NFT Market Place

4.5.1 Description and Priority

In the NFT marketplace, the user can sell or buy vehicles. If the user is a seller, he or she wants to open a request to sell his vehicle, then the NFT of this vehicle is marked as sale. If the user is a buyer, he can see all NFTs which are in the selling state with the price. The benefit of the NFT Market Place is that general users can sell and buy vehicles in a secure manner. If we do not create this part of the project the penalty is that we won't be able to sell or buy vehicles and there is no use of what we did up this by generating NFTs of vehicles and SSIs related to general users.

4.5.2 Stimulus/Response Sequences

Upon logging in with their SSI credentials, the general user is able to view a selection of vehicles available for sale on the home page of NFT Vehicle Marketplace. In the home page there can be seen each vehicle as a card with an image of that vehicle and few details. After clicking on any card, the general user is directed to a page which can be seen all the details (past owners, price, vehicle technical details, vehicle number, etc.) related to that vehicle. There is a separate tab to view the NFTs which belong to that user. There is a separate button to move to the selling pages. And the seller can fill in a few data fields and make a particular NFT available for selling. And if any buyer needs to buy a particular vehicle, that person can click on the vehicle card that he wants to buy. And after clicking there is an option to buy that vehicle and after using that option the buyer can do the transaction using cryptocurrency. And then the transaction happens with the aid of the meta mask wallet and the ownership of the NFT is transferred to the new owner.

4.5.3 Functional Requirements

REQ-14: The system must provide the chance to log in to the marketplace.

REQ-15: The system must provide a facility for all the system users to view a selection of vehicles that are available for sale.

REQ-16: The system must provide a facility to view all the details related to the vehicle which are up to sale.

REQ-17: The system must provide facilities to do the transaction of vehicle using cryptocurrency.

REQ-18: The system must provide the chance to change the ownership of a NFT from a seller to buyer.

REQ-19: The system must provide the chance to view the NFTs belonging to them self through the system.

5. Other Nonfunctional Requirements

5.1 Performance Requirements

The response time would be an important feature when measuring performance. The response time should be low enough so that the user won't be inconvenienced when using the application. Another important feature would be the user-friendliness of the application. The user should not find it difficult or unpleasant to navigate the application.

5.2 Safety Requirements

It's important that any data that we store, especially that of the users, is kept safe from data loss for any reason. The data that is stored in the database should be backed up regularly to ensure that there isn't any loss of data. The backups should be able to restore the data in case of any loss of data. It's also important to maintain the server so that it's kept running and to ensure that it can handle increased data capacity as the number of users increases.

5.3 Security Requirements

The system should have secure authentication and authorization for all users. Each user should log in to the system using usernames & passwords provided by the Organization. In addition, it should have secure communication channels for all data transmission and should have data encryption for all sensitive information.

5.4 Software Quality Attributes

There are several software qualities that would be vital in order to put out quality software. Some of these attributes are,

- Correctness
- Reliability
- Adequacy
- Learnability
- Robustness
- Maintainability
- Readability

- Extensibility
- Testability
- Efficiency

If these qualities are present in software, it can be considered to be of high quality.

5.5 Business Rules

The product can be used by both social influencers and businesses. The user roles for both these users would be almost the same on all occasions. The businesses would have the additional capability of adding projects and events. The administrator is in charge of adding users and ensuring that all reported comments and users are looked into.

6. Other Requirements

When we figured out both international and legal requirements we came across with these requirements. According to that, the SSI which we create for users must have the ability to be used in any situation which we need to verify the identity of that user. And also, the NFT which we mint for a particular vehicle must be accepted in any NFT marketplace. And other than that, there is an international requirement which we need to fulfill. That is our SSI, NFT, and the process going on in the NFT Market Place have to be accepted by any country. And there is an initialization requirement also. That is, the government has to allow permission to deploy our system.

Appendix A: Glossary

List of Abbreviations

| Abbreviation | Meaning |
|--------------|------------------------------------------------------|
| DeFi | Decentralized Financing |
| EIP | Ethereum Improvement Proposals |
| ERC | Ethereum Request for Comment |
| ETH | Ethereum |
| IPFS | Inter Planetary File System |
| NFT | Non-Fungible Token |
| RTA | Road Transport Authority |
| MVT | Model View Template |
| DLT | Distributed Ledger Technology |
| ACA-Py | Aries Cloud Agent Python |
| VOMS | Vehicle Registration and Ownership Management System |
| SRS | Software Requirement Specification |
| QR | Quick Response |
| HTTP | Hypertext Transfer Protocol |
| POC | Proof of Concept |

Appendix B: Analysis Models

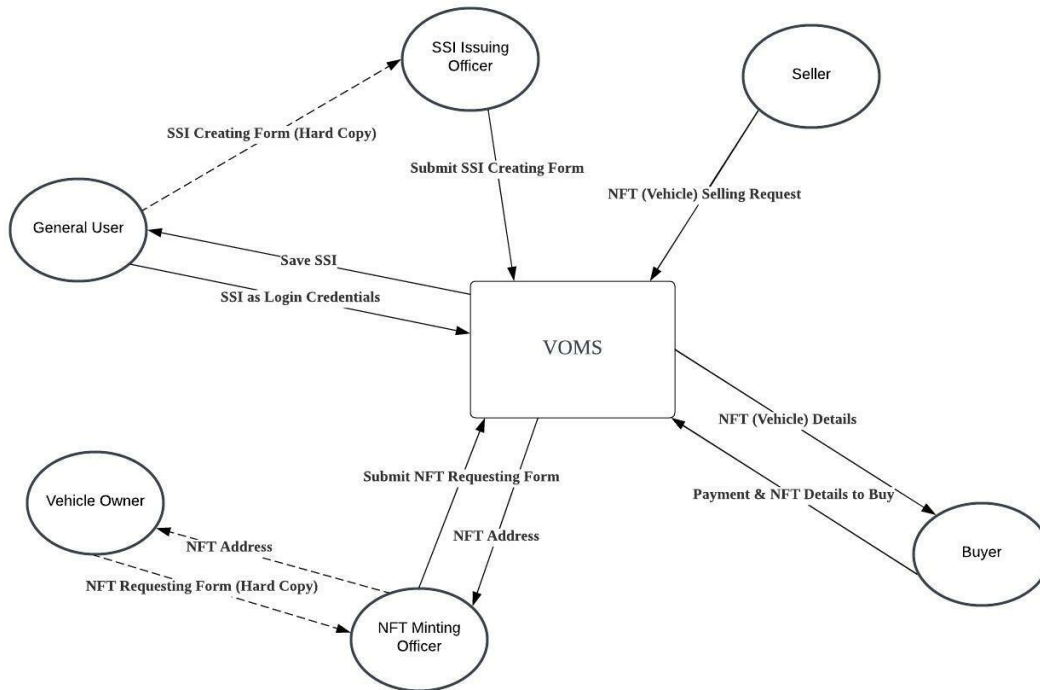


Figure 6-1 Input Output Diagram

Class Diagram

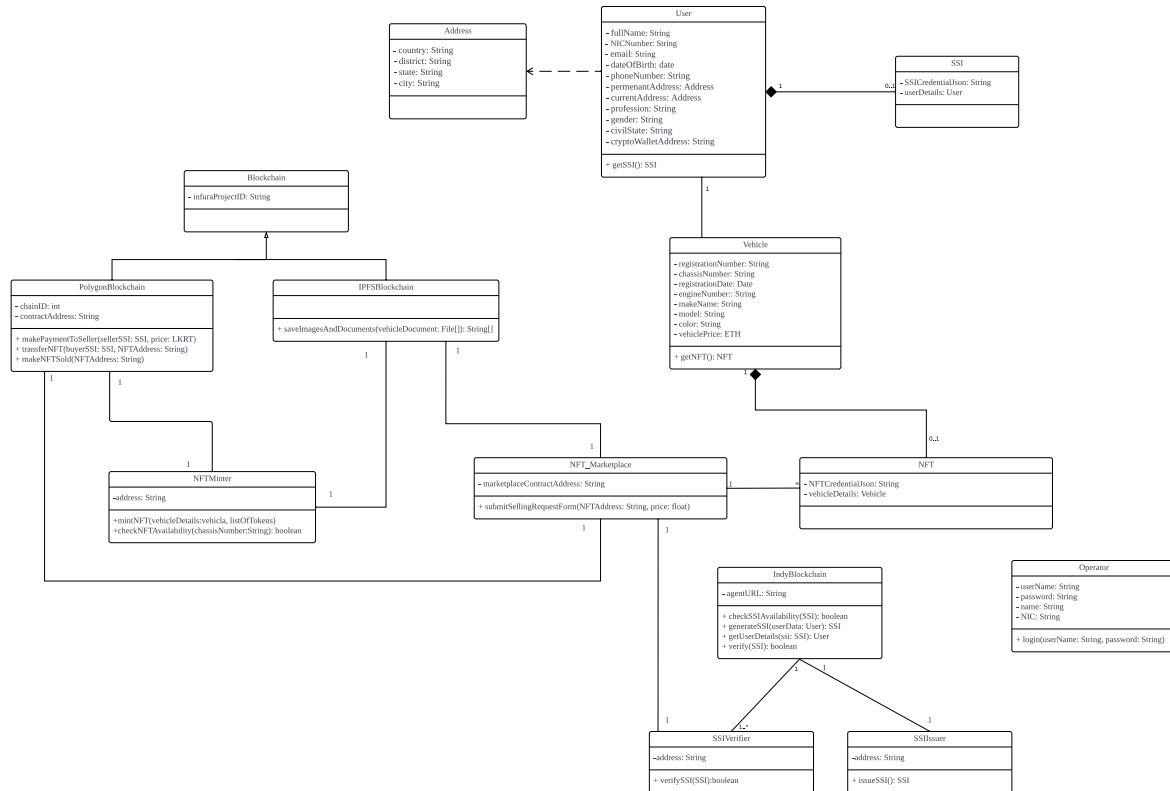


Figure 6-2 Class Diagram

ER Diagram

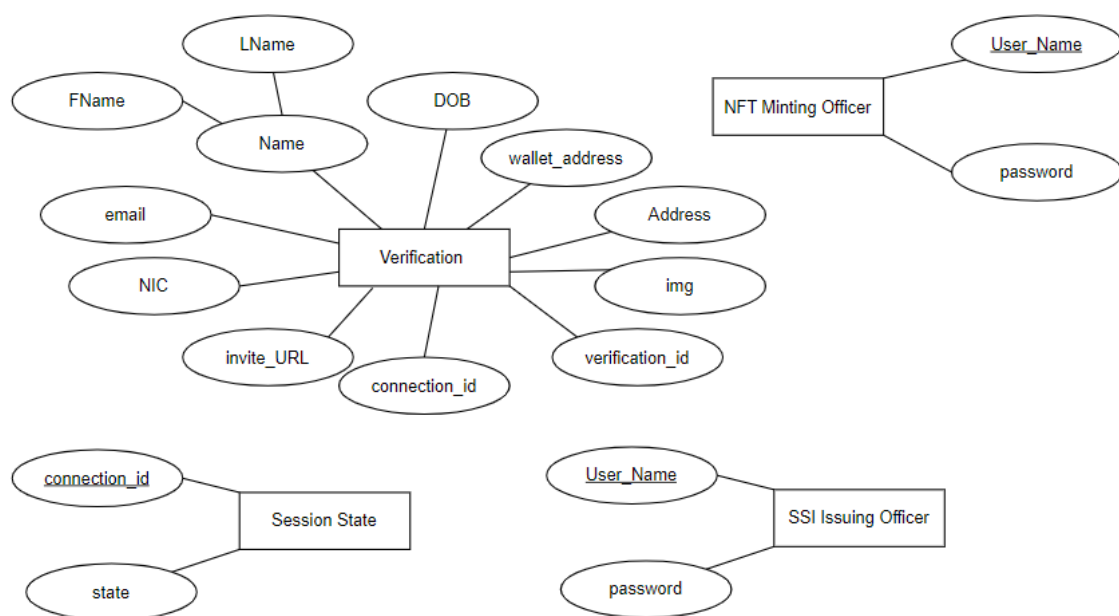


Figure 6-3 ER Diagram