



**ÇANKAYA UNIVERSITY**  
**FACULTY OF ENGINEERING**  
**COMPUTER ENGINEERING DEPARTMENT**

**CENG 407**

**Innovative System Design and Development I Project Report**

**Team ID: 202411**

**ScubaCHAIN: Adopting Blockchain Technology in Scuba Diving**

Deniz KAR - 202011042

Ahmet Berk EROĞLU - 202011411

İclal Sezin GÜRSES - 202111017

Mustafa Arda ERDİNÇ - 202011073

Arda Celal KAPLAN - 202111013

**Advisor: Gül TOKDEMİR**

Table of Contents

Cover Page ..... 1

Introduction ..... 5

Project Work Plan ..... 6

LITERATURE REVIEW ..... 8

Abstract..... 9

1. Introduction..... 10

2. Verification of Scuba Diving Licenses..... 10

    a. Physical Card Verification ..... 10

        i. Advantages: ..... 11

        ii. Disadvantages:..... 11

    b. Centralized Digital Databases ..... 11

        i. Advantages: ..... 11

        ii. Disadvantages:..... 11

    c. Blockchain-Based Verification ..... 11

        i. Advantages: ..... 12

        ii. Disadvantages:..... 13

    d. API Integration with Government or Third-Party Systems ..... 13

        i. Advantages: ..... 13

        ii. Disadvantages:..... 14

    e. Mobile App-Based Verification ..... 14

        i. Advantages: ..... 14

        ii. Disadvantages:..... 14

    f. Near-Field Communication (NFC) Verification..... 14

        i. Advantages: ..... 15

        ii. Disadvantages:..... 15

3. Blockchain ..... 15

    a. Key Characteristics of Blockchain..... 16

    b. How Blockchain Works ..... 16

    c. Applications of Blockchain..... 16

4. Blockchain in Scuba Diving License Verification Systems..... 17

5. Web Programming ..... 18

    a. What is Web?..... 18

    d. Web 2.0 in Our Project..... 19

        i. Front End..... 19

        ii. Back End ..... 20

        i. Decentralization and Data Ownership: ..... 23

6. What is IPFS? ..... 25

    a. How To Use IPFS In Our Project ..... 25

7. What is Flutter? ..... 26

    a. Advantages of Using Flutter ..... 26

8.	What is PADI? .....	26
9.	What is CMAS? .....	26
10.	PADI vs. CMAS .....	27
a.	Why Do We Need a Digital Signature? .....	28
b.	Why Do We Need to Verify Licenses? .....	28
c.	What is OpenZeppelin, and What is Its Purpose? .....	28
d.	Why Should We Use OpenZeppelin in Our Project? .....	28
12.	What is Solidity? .....	29
a.	Advantages of Solidity for Our Project .....	29
13.	Metamask .....	30
14.	Truffle & Hardhat .....	30
	Conclusion .....	32
	<b>SOFTWARE REQUIREMENTS SPECIFICATION .....</b>	<b>33</b>
1.	INTRODUCTION .....	34
1.1.	Purpose .....	34
1.2.	Scope of Project .....	34
1.3.	Glossary .....	36
2.	OVERALL DESCRIPTION .....	38
2.1.	Product Perspective .....	38
2.1.1.	Development Methodology .....	38
2.2.	User Characteristic .....	39
3.	REQUIREMENTS SPECIFICATION .....	40
3.1.	External Interface Requirements .....	40
1.	Diver Interface .....	40
2.	Dive Center and Divemaster .....	41
3.	Common Features .....	42
•	Mobile Application (Front-end): .....	42
•	Server (Back-end): .....	42
•	Blockchain and IPFS Integration: .....	43
3.1.4	Communication Interfaces .....	43
3.2.	Functional Requirements .....	44
3.3	Performance Requirements .....	52
3.4	Software System Attributes .....	53
3.5.	Safety Requirement .....	54
	<b>SOFTWARE DESIGN DESCRIPTION .....</b>	<b>56</b>
1.	INTRODUCTION .....	57
1.1	Purpose .....	57
1.2	Scope .....	57
1.3	Glossary .....	58
1.5	Motivation .....	59
2.	SYSTEM DESIGN .....	60

2.1	Architectural Design.....	60
2.1.1	Problem Description.....	61
2.1.2	Technologies Used .....	61
1.	Blockchain Technology.....	61
2.	Frontend Development.....	62
3.	Backend Development .....	62
4.	Database Management .....	62
5.	Authentication and Identity Management .....	62
2.1.3	Data Flow Diagram (DFD).....	63
3.	USER INTERFACE (UI) DESIGN.....	73
	Conclusion.....	78
	Reference.....	79

# **Introduction**

The ScubaChain project aims to revolutionize scuba diving certification and dive log management by utilizing blockchain technology to enhance security, transparency, and trust within the diving community. The traditional paper-based system in the scuba diving industry poses challenges like data loss, forgery, and limited accessibility. ScubaChain addresses these issues by creating a decentralized digital platform that allows users to securely store and verify their certifications and dive logs using blockchain and IPFS technologies.

This document outlines the design, implementation, and management of ScubaChain, focusing on creating a user-friendly platform for divers, dive masters, and dive centers. The platform includes features such as certification verification, dive log management, interactive maps, and NFT-based rewards to foster engagement and community building within the global diving ecosystem. By leveraging cutting-edge technologies, ScubaChain aims to set a new standard for digital identity and secure data storage in the diving industry.

# Project Work Plan

Start Date 24/10/2024			
Week		Week 1	Week 2
Procedural Steps	Current State	30 September 2024	7 October 2024
Team Setup	Completed		
Project Proposal Form	Completed		
Project Selection Form	Completed		
Project Work Plan	Completed		
Literature Review	Continuing		
Software Requirements Specification	Continuing		
Project Webpage	Continuing		
Software Design Description	Continuing		
Project Report	Continuing		
Presentation	Continuing		

[illegible][illegible]

[illegible]

# **LITERATURE REVIEW**



## **Abstract**

In recent years, blockchain technology has emerged as a groundbreaking solution to enhance data security, transparency, and trust within various industries. This project seeks to leverage blockchain's immutable and decentralized architecture to develop a secure scuba diving certification and dive log management system. Targeting a wide range of users including divers, divemasters, and dive centers this platform aims to standardize and digitize the verification process for diving certifications and dive logs, which are traditionally paper-based and vulnerable to forgery. Through blockchain, digital signatures, and advanced cryptographic verification methods, the project aspires to establish a more accessible and secure way to validate skills, log dives, and manage diving records.

This system encompasses two primary components: a web-based platform, which enables dive centers and divemasters to issue and verify certifications on the blockchain, and a mobile application for divers to access, review, and manage their personal dive records. In addition to basic certification tracking, the platform will incorporate a range of user-centric features: dive event creation, geolocation mapping, weather condition integration, and social media sharing that foster community engagement. Unique to this project is the integration of NFTs, which divers can earn for participating in specific events or achieving milestones, further enhancing user interaction through a gamified approach.

With the potential to transform scuba diving record-keeping into a transparent, trustless, and community-oriented ecosystem, this project not only facilitates secure access to diving certifications but also promotes digital identity and sustainable data storage practices. By utilizing blockchain's strengths in data integrity and transparency, this platform envisions a global and secure dive management system that elevates safety, encourages achievement, and fosters a thriving diving community.

# 1. Introduction

In the quest to digitize and secure data in all aspects of life, scuba diving remains an area where traditional, paper-based practices still dominate. Certification, skill verification, and dive log maintenance largely rely on physical documents, making them vulnerable to loss, forgery, and limited accessibility. Recognizing these issues, ScubaChain introduces a groundbreaking solution: a blockchain-based platform designed to modernize and secure the scuba diving ecosystem. With ScubaChain, divers, divemasters, and dive centers gain access to a reliable, transparent, and tamper-proof system that verifies and tracks diving credentials on an immutable digital ledger.

ScubaChain serves three main user personas: divers, divemasters, and dive centers, each interacting through dedicated interfaces and tools. Dive centers and divemasters can access a secure web-based platform to verify certifications and log dives directly on the blockchain, while divers use a mobile app to manage personal records, register for dives, and access live updates on their certification statuses. Designed to go beyond simple record-keeping, ScubaChain also integrates a range of interactive features such as geolocation-based dive maps, real-time weather and water conditions, and social media sharing options. Together, these elements not only digitize the diving experience but also build a connected and engaged diving community.

## 2. Verification of Scuba Diving Licenses

Ensuring that scuba divers possess appropriate and current certifications is essential for safe underwater activities. License verification in scuba diving is a structured process to confirm the diver's skills, experience, and authorization to dive to certain depths or in particular environments. This process serves to enhance safety for both the divers and dive operations, ensuring that only qualified individuals participate in activities that align with their certified skills.

### a. Physical Card Verification

Traditionally, scuba divers receive a physical certification card after completing their training with recognized diving organizations, such as PADI (Professional Association of Diving Instructors), CMAS (Confédération Mondiale des Activités Subaquatiques), or NAUI (National Association of Underwater Instructors). This physical card contains details such as the diver's name, certification level, issuing organization, and certification date.

**i. Advantages:**

- **Immediate and Tangible Proof:** Divers can carry the card for on-site verification without relying on digital access.
- **Simplicity:** For smaller dive shops, card verification is simple, requiring minimal technological setup.

**ii. Disadvantages:**

- **Potential for Fraud:** Physical cards can be lost, stolen, or even counterfeited, which can lead to unqualified individuals accessing diving services.
- **No Real-Time Updates:** If a diver's status changes (e.g., certification suspension or revocation), the physical card won't reflect this unless replaced, causing potential safety risks.

## **b. Centralized Digital Databases**

With advancements in digital technologies, major diving organizations maintain centralized online databases where dive operators and centers can verify certifications. These databases are accessible via the organization's website or app, allowing divers and operators to validate licenses in real time.

**i. Advantages:**

- **Enhanced Security:** Digital verification reduces the risk of fraud by providing direct access to authoritative records.
- **Real-Time Data:** Centralized databases are frequently updated, allowing verification of the diver's most current certification status.

**ii. Disadvantages:**

- **Access Dependency:** Verification relies on internet connectivity, which may not be available in remote locations.
- **Privacy Concerns:** Data storage on a central server raises questions about data privacy and the potential for unauthorized access.

## **c. Blockchain-Based Verification**

Blockchain technology offers an innovative approach to certification verification, ensuring data immutability, transparency, and decentralized access. In a blockchain-based system, certification information is stored on a distributed ledger, which can be accessed by dive centers, instructors, and divers without relying on a centralized

database. Each certification could be digitally signed, timestamped, and recorded on the blockchain, providing a tamper-proof record of the diver's credentials.

i. **Advantages:**

- **Secure and Immutable Records:** Blockchain's primary advantage lies in its ability to securely and immutably store data, which ensures that critical data, such as scuba diving licenses, is protected against unauthorized modifications. Once recorded, license data is tamper-proof, allowing users and authorities to view the history of records with confidence.
- **Decentralization:** Blockchain operates without dependence on a central authority, meaning that multiple centralized authorities are unnecessary for the verification of diving licenses. As a result, license holders benefit from a reliable and independent system for verification and record-keeping without the need for a singular controlling entity.
- **Digital Identity and Ownership Proof:** Blockchain enables digital identity verification and ownership proof through digital signatures, allowing divers to store their certifications digitally and present them conveniently. This eliminates the need for physical certificates, streamlining verification through digital identity and ownership.
- **Data Transparency:** Blockchain's transparency allows all registered data to be accessible to relevant parties, facilitating easy verification of divers' licenses by all stakeholders. This transparency strengthens trust among users and regulatory authorities by ensuring the integrity of license data.
- **Automated Certification and Updates:** By leveraging smart contracts, certification processes can be automated. For instance, a diver reaching a specified number of dives can automatically qualify for an advanced level, minimizing human errors, expediting license upgrades, and reducing costs.
- **Secure Storage of Dive Logs:** Dive history and logs can be securely stored on the blockchain, enabling reliable verification of a diver's experience. This feature is especially valuable when divers present their logs to new dive centers, as it guarantees the authenticity of their past dives.
- **Cross-Platform Compatibility:** A blockchain-based system can integrate license data from various certification organizations (e.g., PADI, CMAS), allowing unified license verification through a single blockchain system. This fosters compatibility across different certification bodies.

ii. **Disadvantages:**

- **High Costs:** Blockchain systems require significant development and maintenance costs, especially if a private blockchain is created or the system is built on an existing blockchain network. Compared to traditional systems, the initial setup costs are notably higher.
- **Data Privacy Concerns:** Due to blockchain's transparency, user data, such as dive logs, may be visible to the public. Ensuring the privacy of personal data can be challenging, potentially causing trust issues among users.
- **Energy Consumption:** Some blockchain types, particularly those using Proof of Work (e.g., Bitcoin), consume high amounts of energy, which is environmentally unfavorable. This energy demand impacts both the environmental sustainability and financial feasibility of such projects.
- **Security Risks:** While blockchain records themselves are secure, vulnerabilities may exist in the smart contracts or system integrations used. If a smart contract contains security flaws, malicious actors could manipulate data or disrupt the system.
- **Irreversible Transactions:** Transactions on the blockchain are irreversible, meaning incorrect data entries cannot be rectified. Any erroneous license or dive record remains permanently on the system, potentially creating issues for the user.
- **Lack of Regulation:** Blockchain-based digital identity verification and certification systems are not yet widely recognized by regulatory authorities in many countries. Without formal recognition, certifications may face challenges in gaining acceptance at dive centers and could lack official validity.

## **d. API Integration with Government or Third-Party Systems**

Some countries or regions may have government-mandated diving regulations and license databases. API integration allows dive operators to connect with these official databases to verify certifications directly. For instance, in certain countries, CMAS certifications can be verified through government APIs.

i. **Advantages:**

- **Official and Verified Sources:** Access to government or certified third-party databases ensures authenticity and compliance with local regulations.
- **Automated Verification:** APIs can allow automated verification workflows, streamlining the process for large diving operations.

ii. **Disadvantages:**

- **Geographic Restriction:** API integration is often specific to one country or region, limiting its applicability in international diving contexts.
- **Data Access and Privacy Issues:** Accessing government databases may involve strict privacy policies and restrictions, which can complicate data retrieval processes.
- 

**e. Mobile App-Based Verification**

Some diving agencies offer mobile applications that store digital versions of certifications. Divers can use these apps to show their credentials, which can be validated through QR codes, RFID technology, or direct database access within the app itself.

i. **Advantages:**

- **Convenience:** Divers can carry their credentials on their smartphones, eliminating the need for physical cards.
- **Interactive Features:** Some apps include additional features like tracking dive logs, certification renewals, or even sharing dive experiences.

ii. **Disadvantages:**

- **Dependence on Device Availability:** If a diver's smartphone is lost or out of power, they cannot access their certification data.
- **Security Concerns:** Apps may be susceptible to hacking if not properly secured, leading to potential fraud or data breaches.

**f. Near-Field Communication (NFC) Verification**

NFC-enabled certification cards or tags allow divers to tap their cards against an NFC-enabled device, which then retrieves certification data. This method can be particularly useful at diving facilities, where verification can be automated with NFC readers.

**i. Advantages:**

- **Quick and Contactless:** NFC technology allows rapid and hygienic verification without needing direct physical interaction.
- **Offline Verification Capability:** Certain NFC tags can be preloaded with data, allowing offline verification in areas without internet access.

**ii. Disadvantages:**

- **Infrastructure Requirements:** Dive centers need to have NFC-enabled devices, which may be a barrier for some.
- **Data Storage Limitations:** NFC tags have limited storage, so they may not be able to hold full certification records.

In summary, each verification method offers unique strengths and limitations that suit different operational needs and diving environments. Traditional physical cards are simple but vulnerable to fraud, while centralized databases and APIs provide secure, real-time access but depend on connectivity. Blockchain-based systems offer a groundbreaking level of security and accessibility, though they require significant investment. Mobile apps and NFC technology improve user convenience and speed but come with limitations regarding device reliance and data storage.

Combining multiple verification methods may yield the best balance of security, accessibility, and reliability in scuba diving license verification. As the industry evolves, technology will continue to play a critical role in ensuring that divers meet safety standards, helping create a secure and trustworthy environment for divers and dive centers worldwide.

### **3. Blockchain**

Blockchain is a type of distributed digital ledger technology (DLT) that securely records transactions and data across multiple computers in a network. Essentially, it's a database that's shared among a network of computers, called "nodes," and it organizes information into "blocks" of data that are then "chained" together. This makes it nearly impossible to alter or delete any single record without altering all subsequent records, providing security and transparency.

## a. Key Characteristics of Blockchain

- i. **Decentralized:** Instead of being stored in a single, central location (like a traditional database), copies of the blockchain exist on multiple nodes within the network. No single entity has complete control.
- ii. **Immutable:** Once data is recorded in a block, it cannot be changed without changing all the subsequent blocks, which would require agreement from the majority of the network. This makes the data on a blockchain tamper-resistant.[9]
- iii. **Transparent:** All transactions recorded on the blockchain are visible to all participants in the network, which promotes transparency and trust.
- iv. **Consensus Mechanism:** To validate transactions and add new blocks, most blockchains use consensus mechanisms like Proof of Work (used by Bitcoin) or Proof of Stake (used by Ethereum 2.0 and other platforms) to ensure that all participants agree on the contents of the blockchain.

## b. How Blockchain Works

- i. **Transaction Creation:** A user initiates a transaction, like sending cryptocurrency to another user.
- ii. **Verification:** Nodes in the network verify the transaction to ensure it's legitimate.
- iii. **Block Formation:** Verified transactions are grouped into a block.
- iv. **Consensus:** The network's consensus mechanism verifies the new block.
- v. **Chain Addition:** Once approved, the block is added to the existing blockchain in chronological order.
- vi. **Immutable Record:** The transaction is now part of the blockchain, viewable and verifiable by all network participants.

## c. Applications of Blockchain

- i. **Cryptocurrency:** Blockchain is the underlying technology for cryptocurrencies like Bitcoin and Ethereum.
- ii. **Supply Chain Management:** It can track the origin, movement, and handling of goods, enhancing transparency and reducing fraud.
- iii. **Finance:** Blockchain can improve the speed, security, and transparency of financial transactions.
- iv. **Healthcare:** It can securely store patient records, ensuring privacy and enabling easy sharing across providers.



- v. **Smart Contracts:** Self-executing contracts that automatically enforce the terms of an agreement when certain conditions are met.

## 4. Blockchain in Scuba Diving License Verification Systems

The integration of blockchain technology into scuba diving license verification systems represents a transformative approach to ensuring transparency, security, and reliability. Traditionally, license verification relies on physical documentation or centralized databases, which are susceptible to tampering, loss, or data inaccuracies. Blockchain, with its immutable and decentralized nature, provides a robust solution to these challenges by creating a tamper-proof digital ledger where dive certifications and other credentials can be securely stored and verified.

A blockchain-based license verification system offers divers a secure way to manage and share their certifications digitally, eliminating the need for physical copies. Each certification can be digitally signed and recorded on the blockchain, creating an indelible record that accurately reflects a diver's current status and skill level. This approach not only enhances data security but also allows dive centers and instructors to quickly verify certification details, improving efficiency in dive operations.

Furthermore, such a system can serve as a unified platform that accommodates certifications from multiple international organizations, including PADI and CMAS. By incorporating these global standards into a decentralized network, blockchain facilitates a universally recognized credentialing framework. This would allow divers to have their certifications verified seamlessly across various jurisdictions and dive centers, fostering a more cohesive, trustworthy global dive community.

The potential benefits extend beyond individual verification; blockchain enables secure and efficient access to certification data for all relevant parties, significantly reducing administrative burdens. This innovation aligns with the dive sector's shift toward digitization, enhancing overall safety standards by providing rapid access to accurate information about divers' qualifications. Thus, blockchain's application in license verification for scuba diving could mark a pivotal advancement in promoting standardized, secure, and accessible digital credentials within the diving industry.

## **5. Web Programming**

### **a. What is Web?**

The World Wide Web, often referred to as WWW, W3 or the Web, is a system of public web pages linked together and we can access the pages using the internet. The Web is not the same as the Internet: The web, which is the most important of the applications built on the Internet, is very important for people. Tim Berners-Lee proposed the architecture of the web at CERN in 1989. Tim Berners-Lee built the first web server, web browser and web page in 1990 using his personal computer at CERN. alt.hypertext, a news group created in 1987, is a forum where the concept and applications of hypertext are discussed. Tim Berners-Lee announced his work on the alt.hypertext newsgroup in 1991. The development of the web has been divided into different versions based on the features it offers to users. These are Web 1.0, Web 2.0 and Web 3.0.[3]

### **b. WEB 1.0**

Web 1.0 refers to the first phase in the evolution of the World Wide Web and lasted from roughly 1991 to 2004. Personal web pages were quite common on the Internet during this period, but they had only a limited number of content creators. Placing ads on websites was prohibited, so users would have an ad-free experience while browsing the internet. During the Web 1.0 era, digital photography sites like Ofoto allowed users to store, share, view and print their digital photos. In this period, which was suitable for the use of personal websites, there was a certain cost per page viewed. Its advantage is that it is simple and fast. The disadvantage is that interaction with users is low and one-way.

### **c. WEB 2.0**

The term Web 2.0 was first coined by Darcy DiNucci in 1999, but became popular in 2004 with the First Web 2.0 Conference organized by Tim O'Reilly and Dale Dougherty. Web 2.0 refers to a period in which users can produce and share content, aiming to provide an interactive internet experience. With platforms such as blogs, social media sites and forums, users are now not only consumers of information but also producers of content.

While the advantages of Web 2.0 are high interactivity, user-generated content and social sharing, its disadvantages include data privacy and security risks. This structure has transformed the internet into a more social and dynamic platform.

## **d. Web 2.0 in Our Project**

Web 2.0 technologies allow you to actively interact with users, involve them in the project and provide a more interactive experience. Instead of just viewing content, users have the opportunity to contribute, share and participate in the project. If user interaction, social sharing and personalization are important in the project, Web 2.0 enhances this experience, increasing user interest and promoting loyalty.

### **i. Front End**

The front-end is the face that users directly interact with on a website or app. This area covers all the visual elements that shape the appearance and user experience of the site. The front-end, created with technologies such as HTML, CSS and JavaScript, is optimized in terms of aesthetics and functionality and aims to offer an interface where users can easily navigate and find information easily. Responsive design and performance optimization are also important elements of the front-end development process.

HTML (Hypertext Markup Language) is a markup language used to create the architecture of web pages and determines how content will be presented to the user. It defines how elements such as headings, paragraphs, texts, links and images are arranged on the page, thus forming the main framework of web pages.

CSS (Cascading Style Sheets) is a style language used to determine the visual layout of web pages. It is applied to add aesthetics to pages created with HTML and gives the desired appearance to the page by controlling visual elements such as color, font and layout.

JavaScript is a programming language used to add interactivity and dynamic features to web pages. It can respond to user actions; for example, it can display a message when a button is clicked or verify data when filling out a form. Thanks to this functionality, JavaScript makes web pages more user-friendly and interactive.

React, Vue.js, Ember.js, Backbone.js and AngularJS, which are widely used to develop user interfaces and especially single-page applications,

are the prominent tools. React was developed by Facebook and focuses on interactive interfaces, while Vue.js offers a smoother and more accessible syntax. AngularJS, provided by Google, stands out with its powerful features for creating dynamic and complex interfaces

React.js is a JavaScript library developed by Facebook and is popular for creating dynamic and fast user development. It is a fun and beautiful alternative to single page applications (SPAs) and mobile applications. React offers a base-based structure, allowing you to manage and reuse the different sections presented as independent parts. In this way, it helps user interactions and visual organization in a more orderly manner. User security provides both comfort and fast service.

- Using the Virtual DOM, React quickly learns about updates and updates the components that need to be updated, thus increasing performance.
- It responds to user interactions faster than its competitors thanks to its Virtual DOM and component-based structure
- It has many libraries. Therefore, it quickly responds to various development needs.
- Pages developed with React can be processed on the server side, allowing search engines to access them much faster
- Since JSX (JavaScript XML) provides a syntax similar to HTML, developers with HTML and JavaScript knowledge can easily learn React.
- Using a single code base simplifies the process of developing mobile applications, allowing them to run seamlessly across multiple platforms. This approach reduces the need for separate code for each platform, making development faster and more efficient.

## **ii. Back End**

The backend, also known as the server-side, is essential in web and mobile applications for managing data processing tasks and ensuring frontend functionality. This layer is responsible for critical operations such as database management, user authentication, and data storage. Backend development encompasses the design and implementation of the application's underlying logic and infrastructure, focusing on tasks like security protocols, deployment strategies, and performance optimization, all of which support a seamless user experience on the client-side.

- **Node.js**

When a client sends a request from the client side of an application, it is forwarded to the server for validation, where necessary processing and calculations occur. Following this validation, the server responds to the client. Node.js, a popular JavaScript framework, is used to manage these server-side operations efficiently.[1]

As an open-source, cross-platform JavaScript runtime, Node.js enables web applications to run independently of the client's browser, making it ideal for executing server-side applications. Its efficient design is particularly suitable for creating I/O-intensive applications like video streaming services, chat platforms, and other real-time, data-driven applications. Due to its robust performance and flexibility, Node.js has gained significant traction, being adopted by both large tech companies and innovative start-ups to power their backend infrastructure.

- **Express.js**

Express is a framework built on Node.js that significantly streamlines the development of web and mobile applications. It supports single-page, multi-page, and hybrid applications, simplifying server management and routing processes.[2] By reducing coding time, Express enhances efficiency in API development, making it an ideal choice for creating robust applications with fewer resources. Its foundation in JavaScript makes it accessible for beginners, facilitating entry into web development for those without extensive programming experience. Key reasons for the widespread adoption of Express include its speed, time efficiency, cost-effectiveness, and support for asynchronous operations, all of which contribute to its value in modern web application development.

- **PostgreSQL**

PostgreSQL is a robust open-source object-relational database management system, known for its high performance, rich features, and adaptability, developed over more than 35 years. It enables developers and administrators to handle datasets of all sizes, ensuring data integrity and stability. PostgreSQL's extensible architecture allows the addition of

custom data types, functions, and supports multiple programming languages without needing recompilation.

On the other hand, MongoDB is a NoSQL document-based database that offers excellent flexibility and scalability, especially for managing complex or unstructured data. Unlike PostgreSQL, which organizes data in structured tables, MongoDB utilizes JSON-like documents that allow for fast data retrieval and easy replication. While both databases are ACID-compliant, PostgreSQL is often favored for structured data, whereas MongoDB is more suitable for dynamic and flexible data models.

## **e. WEB 3.0**

Web 3.0, or Web3, is the third generation of the World Wide Web and promotes blockchain technology and cryptocurrencies while emphasizing personal data ownership. This internet version, which is still in the early stages of development, provides a more open and decentralized platform. The aim of Web 3.0 is to create an internet structure that users can control and can perform peer-to-peer transactions without being dependent on authoritarian places. Web 3.0 technologies are anticipated to be decentralized, trustworthy, and fully transparent, with content creation platforms expected to be built upon open-source technologies to ensure accessibility and transparency. By applying Zero Trust principles, Web 3.0 aims to achieve maximum network security in an environment where trust is not presumed. This approach enables users, devices, and services to interact directly without requiring authorization from a central authority, promoting a secure and autonomous digital ecosystem.

With blockchain technology, the next phase of the internet will enable individuals to communicate directly and without intermediaries. Users can connect by joining Decentralized Autonomous Organizations (DAOs), which are governed and owned by communities, allowing them to participate actively in decision-making processes. The security of user data will be ensured through a network of public smart contracts operating on a blockchain, managed by a decentralized node network rather than central authorities. Consequently, user data will be stored in a more secure and transparent environment.

Web 3.0 projections indicate that blockchain technology will facilitate decentralized data transfers by recording all transactions on a distributed ledger, thereby creating a more transparent and secure data environment. This approach

reduces reliance on centralized authorities for maintaining data integrity, as open smart contracts will manage this responsibility autonomously. Additionally, the metaverse is anticipated to drive substantial revenue growth in the entertainment industry, reshaping how users engage with digital content and immersive experiences. Blockchain will also enhance the protection of intellectual property and personally identifiable information (PII), empowering users to control their personal data more effectively. At the same time, users will have the capability to swiftly create digital assets and non-fungible tokens (NFTs), fostering new avenues for creativity and ownership. Furthermore, individuals will be able to monetize their own data, marking a shift in power that provides both control and financial benefits directly to users, rather than centralized entities.

In the context of the scuba diving license verification project ScubaChain, Web 3.0 plays a transformative role by introducing decentralized, user-centric features that make use of blockchain technology, digital identity systems, and smart contracts. These elements collectively enhance security, interoperability, and user control over data, making the verification process more efficient, transparent, and globally accessible.

i. **Decentralization and Data Ownership:**

At its core, Web 3.0 facilitates the decentralization of data, allowing users (divers, dive centers, and certification authorities) to directly own and control their data. In the traditional Web 2.0 model, data ownership is primarily centralized, held by specific authorities or platforms. With Web 3.0, each diver's license information, including certification level, dive history, and achievements, can be securely stored on a public blockchain. This decentralization not only reduces dependency on any central authority but also ensures that records are tamper-proof and accessible globally, enhancing trust and transparency.

ii. **Digital Identity and Verification:** Web 3.0 integrates digital identity solutions, where divers can establish verifiable credentials that serve as digital representations of their licenses. Through blockchain technology, each diver's digital identity is linked to their certification records in a decentralized and encrypted manner. This provides divers with a secure, portable identity that they can use across different dive centers and certification bodies without needing to carry physical proof. Web 3.0 allows for self-sovereign identity systems, meaning divers

have complete control over when and with whom they share their information.

- iii. **Interoperability across Platforms:** Web 3.0 promotes interoperability by enabling various certification authorities (such as PADI, CMAS, etc.) to coexist on the same blockchain. This ensures a unified verification system that dive centers around the world can rely on, regardless of the specific certifying body. Dive centers can quickly verify a diver's credentials across multiple certification organizations, promoting universal recognition of diving qualifications.
- iv. **Smart Contracts for Automated Processes:** Smart contracts play a central role in automating processes within the ScubaChain platform. These self-executing contracts on the blockchain allow dive log entries to be automatically recorded upon meeting certain conditions. By leveraging Web 3.0's smart contract capabilities, ScubaChain minimizes human error, increases operational efficiency, and reduces administrative costs, creating a streamlined user experience.
- v. **Enhanced Transparency and Security:** A defining feature of Web 3.0 is the transparency it brings to data transactions. All information recorded on the blockchain is immutable and can be audited in real time by relevant stakeholders, including divers and regulatory bodies. This transparency fosters trust and accountability within the scuba diving community, as users have assurance that their certifications cannot be tampered with. Additionally, blockchain's cryptographic security protocols in Web 3.0 safeguard personal data against unauthorized access, making it resilient against cyber threats.
- vi. **Cross-Border Accessibility:** Web 3.0's global, borderless nature allows ScubaChain to offer universal access to certification verification. This is particularly beneficial in scuba diving, an inherently international activity, where divers may need to verify their certifications at dive sites worldwide. A Web 3.0-enabled platform like ScubaChain ensures that divers can seamlessly present their verified credentials without encountering regional barriers, enhancing the global scalability and accessibility of the system.



- vii. **Tokenization and Incentives:** Although ScubaChain does not include NFT achievements, Web 3.0 enables tokenization possibilities where divers can be incentivized for regular diving activities or safety practices. While optional for ScubaChain, such tokenization could increase user engagement by rewarding divers with blockchain-based tokens for meeting diving milestones.

By integrating Web 3.0 technologies, ScubaChain introduces a user-centric, secure, and globally scalable solution to the scuba diving industry. This integration not only modernizes the process of license verification but also sets a new standard for how critical certification data can be handled securely, transparently, and efficiently. The shift to Web 3.0 ultimately supports the broader goal of building a decentralized, interoperable, and user-governed ecosystem that could reshape trust and efficiency in scuba diving certification verification

## 6. What is IPFS?

IPFS (Inter Planetary File System) is a distributed, peer-to-peer file storage and sharing protocol. Its primary purpose is to create a decentralized way to store and access files, websites, and applications, moving away from the traditional centralized client-server model. It was developed by Protocol Labs and is often described as a “distributed file system.”[7]

### a. How To Use IPFS In Our Project

- i. **NFT Creation (Minting):** When creating an NFT, you are essentially minting a unique token on a blockchain (such as Ethereum, Solana, etc.) that represents ownership of a specific asset (like an image, video, or other digital content). The key components involved in minting an NFT are:

Metadata: Information about the NFT, such as its name, description, and attributes.

Media Files: The actual content (image, video, music, etc.) associated with the NFT.

In most cases, the metadata and media files themselves are not stored directly on the blockchain because storing large files directly on-chain is costly and inefficient. Instead, IPFS is used to store these files in a decentralized way, ensuring that the NFT's content remains immutable and accessible over time.

- ii. **Storing NFT Metadata on IPFS:** When you mint an NFT, the metadata (which includes information about the NFT) is usually stored off-chain, often on IPFS. This metadata includes:

- The title or name of the NFT

- Description of the NFT or the digital asset it represents
- Attributes or properties of the NFT (for example, the rarity of traits in generative art or a collectible)
- Link to the media (image, video, audio) associated with the NFT

## 7. What is Flutter?

Flutter is an open-source UI (User Interface) software development kit (SDK) created by Google. It allows developers to build cross-platform applications (i.e., apps that work on multiple platforms like Android, iOS, web, and desktop) using a single codebase. This means that with Flutter, you can write your app's code once, and then run it on multiple platforms without needing to rewrite code for each one.

### a. Advantages of Using Flutter

- i. Cross-Platform Development: Save time and resources by building for multiple platforms from a single codebase.
- ii. Consistent UI Across Platforms: Flutter renders its own UI components, meaning your app will look and perform the same across different devices.
- iii. Fast Development: Hot reload and an extensive widget library make it easier and faster to develop, test, and deploy.
- iv. Backed by Google: Flutter has strong support from Google and an active community, with continuous improvements and a growing ecosystem.[8]

## 8. What is PADI?

PADI (Professional Association of Diving Instructors) is one of the world's largest and most recognized organizations for scuba diving training and certification. Founded in 1966, PADI provides a range of scuba diving courses and certifications for beginners, recreational divers, and professionals.

## 9. What is CMAS?

CMAS (Confédération Mondiale des Activités Subaquatiques), also known as the World Underwater Federation, is an international organization that offers training and certification for scuba diving and other underwater sports. Established in 1959, CMAS is

one of the oldest diving certification agencies, and it was founded by Jacques-Yves Cousteau, the famous French underwater explorer, along with representatives from various national diving federations.

## 10. PADI vs. CMAS

Level Type	PADI	CMAS
Entry Level	Scuba Diver, Open Water Diver	One-Star Diver
Intermediate Level	Advanced Open Water Diver	Two-Star Diver
Advanced Level	Rescue Diver	Three-Star Diver
Highest Non-Professional	Master Scuba Diver	Three-Star Diver
First Professional Level	Divemaster	Three-Star Diver (also leadership level)
Instructor Levels	Assistant Instructor, OWSI, MSDT	One-Star, Two-Star, Three-Star Instructor
Technical Diving	TecRec (Tec 40, 45, 50, Trimix)	Mixed Gas, Deep Diving, Cave Diving
Specialties	20+ specialties (e.g., Nitrox, Wreck)	Various specialties, plus scientific diving
Unique Activities	Project AWARE (environmental focus)	Underwater Sports (hockey, rugby, etc.)

## 11. Digital Signature: A Method to Verify Data Integrity and Authenticity

A digital signature is a cryptographic method used to verify the integrity and authenticity of data. It confirms that a piece of data originates from a specific source and has not been altered. Typically, a digital signature is created with a private key and can only be verified with the corresponding public key. This way, anyone who sees the digital signature can be assured that the data comes from a trusted source and has not been tampered with.

## **a. Why Do We Need a Digital Signature?**

In our project, we use digital signatures to ensure the accuracy and source of licenses. A digital signature allows us to verify whether a license is from a legitimate source and if it has been modified. This security measure prevents the use of invalid licenses from external sources, ensuring the safety of our users.

## **b. Why Do We Need to Verify Licenses?**

Verifying licenses guarantees that the software and services used in our project comply with specific rules. This helps prevent copyright infringements and ensures that the software components used in the project are secure. Especially in open-source or license-based projects, using unverified software without valid licenses can lead to legal and security issues. Verified licenses make the project more sustainable and secure.

## **c. What is OpenZeppelin, and What is Its Purpose?**

OpenZeppelin is an open-source library used to develop secure smart contracts on Ethereum and other blockchain platforms. It includes widely-used security protocols for smart contracts and provides security features such as digital signatures, authentication, and access control. For developers writing code in Solidity, it offers various modules that enhance security standards and functionality.[4]

## **d. Why Should We Use OpenZeppelin in Our Project?**

OpenZeppelin provides a strong foundation for security, offering a reliable and tested infrastructure that enhances security in projects. It reduces the likelihood of errors in critical security processes, such as digital signing and authentication. Additionally, as a widely adopted library in the community, security vulnerabilities are quickly identified and resolved. By using OpenZeppelin in our project, we can:

- Conduct digital signature and license verification securely.
- Accelerate the development process by leveraging secure, tried-and-tested libraries.
- Build a structure that complies with smart contract development standards.

Therefore, the digital signature functionality provided by OpenZeppelin will enhance the reliability of our project and strengthen our license management process.

## 12. What is Solidity?

Solidity is a programming language used to develop smart contracts on blockchain platforms such as Ethereum. Solidity is used to write contracts that work securely and transparently on the blockchain, cannot be altered, and are visible to everyone.[5] These contracts, which operate on the blockchain, can automatically execute when certain conditions are met.

### a. Advantages of Solidity for Our Project

Solidity is specifically designed for developing blockchain-based applications and offers several advantages to the project:

- **Security and Transparency:** Smart contracts that run on the blockchain have a reliable structure. Contracts written with Solidity operate within specific rules and are protected against external interference. Since all transactions are recorded on the blockchain, it ensures transparency and can be verified by anyone.
- **Immutability and Reliability:** Smart contracts published on the blockchain are immutable. This feature adds trust to the project and ensures that data and transactions cannot be altered retroactively. This is especially beneficial for processes like digital licensing and ownership verification.
- **Automation:** Smart contracts can automatically execute when certain conditions are met, allowing transactions to proceed without manual intervention. For example, digital license verification processes can be automated through Solidity.
- **Distributed Structure and Decentralization:** Applications built with Solidity can operate on the blockchain without needing a central authority. This enhances reliability and minimizes disruptions and security vulnerabilities that can occur in centralized systems.
- **Community Support and Broad Ecosystem:** Solidity is widely used and continuously developed by the Ethereum community. With a broad range of libraries and tools, it becomes easier to find ready solutions for your project.
- **Tokenization and Financial Transactions:** Solidity supports creating and managing cryptocurrency and tokens if your project requires these features. It enables transactions on the blockchain, making financial processes more secure and traceable.[6]

## 13. Metamask

Users may store and exchange cryptocurrencies, engage with the Ethereum blockchain ecosystem, and host an expanding number of decentralized applications (dApps) with MetaMask, a free web and mobile cryptocurrency wallet. It is among the most popular cryptocurrency apps worldwide. Storage, swaps, and dApp access are the three main applications for MetaMask. When taken as a whole, these features include everything a typical cryptocurrency user would probably require in order to communicate with Ether.

Additionally, anyone may safely expand MetaMask's functionality and create new web3 end user experiences with the help of the open source MetaMask Snaps framework. For instance, a Snap can use its own APIs to add support for several blockchain networks, create unique account kinds, or offer extra features. This makes it possible to utilize MetaMask with a far wider range of protocols, dapps, and services[10]. Metamask features are;

- Actions can be scheduled to execute on a regular basis at predetermined times or intervals; these are referred to as "cron jobs." For instance, you can set MetaMask to show a dialog or notification at a particular time every day.
- Makes Ethereum Virtual Machine (EVM) accounts unique.
- Reverse resolution and custom domain resolution can be used.
- Can be used either unencrypted storage for non-sensitive data or encrypted storage for sensitive data in a Snap.
- When a user installs or updates a Snap, it may utilize lifecycle hooks to have an action, like showing a notification or dialog, execute automatically.
- It can localize your Snap so that the user interface (UI) text and textual metadata (such the title and description) are shown and customized in the user's native tongue.
- With their consent, it is able to use Snaps API methods to manage users' non-EVM accounts and assets.
- Before a user signs a communication, it can offer signature insights. Alerts the user about dangerous signature requests, for instance.
- Snap bundles allows you to manage static files.
- Before a user signs a transaction, it can offer transaction insights via MetaMask's transaction confirmation box. The percentage of petrol fees the user would pay for their transaction, for instance, may be displayed to them.[11]

## 14. Truffle & Hardhat

While testing and creating a blockchain application, The importance and efficiency of the tools used come into play. Truffle and Hardhat are development environments for blockchain apps.

Truffle is development environment, testing framework and asset pipeline for blockchains using the Ethereum Virtual Machine (EVM), aiming to make life as a developer easier. With Truffle, it gives:

- Built-in smart contract compilation, linking, deployment and binary management.
- [Sufficient debugging](#) with breakpoints, variable analysis, and step functionality.
- Use [console.log](#) in your smart contracts
- Deployments and transactions through MetaMask with [Truffle Dashboard](#) to protect your mnemonic.
- External script runner that executes scripts within a Truffle environment.
- Interactive console for direct contract communication.
- Automated contract testing for rapid development.
- Scriptable, extensible deployment & migrations framework.
- Network management for deploying to any number of public & private networks.
- Package management with NPM, using the [ERC190](#) standard.
- Configurable build pipeline with support for tight integration.[12]

Hardhat differs from Truffle. Even Hardhat has same mission with Truffle, it has different work principles:

- Debugging first: The best option for debugging Solidity is Hardhat. When a transaction fails, it provides descriptive error messages, console.log, and Solidity stack traces.
- Exceptional adaptability: It can alter everything you want. Even whole unconventional chores, or portions of them. Design that is adaptable and changeable with little limitations.
- Designed to facilitate integrations, Hardhat enables deeper interoperability between your current tools while letting you continue to use them.
- Fully extensible: With all the tools are needed to meet any project-specific requirements, Hardhat is a tooling platform made to be expanded.
- Plugin ecosystem: Utilize a modular ecosystem of plugins to expand Hardhat's functionality and incorporate your current tools into a seamless workflow.
- Fast iteration: This keeps projects moving forward by increasing the speed of your development feedback loop by up to ten times.

- TypeScript Catching: Use a typed language to detect errors before your code is even executed. TypeScript is fully supported natively by Hardhat.[13]

## Conclusion

In an era where digital transformation is reshaping every industry, ScubaChain offers a groundbreaking approach to the scuba diving community—a sport that values adventure, safety, and a shared connection to the underwater world. By harnessing blockchain technology, ScubaChain aims to provide a secure solution for managing certifications and dive logs, ensuring a trustworthy ecosystem where divers, dive centers, and divemasters can collaborate seamlessly. This approach not only enhances trust but also fosters a system of transparency and verification that is vital for safe diving practices.

ScubaChain's design is rooted in the specific needs of the diving community, addressing both novice and experienced divers while supporting dive centers in their operational needs. By digitizing and securing certifications, ScubaChain creates a standardized framework that can be easily accessed and verified worldwide. This will not only encourage more accountability within the industry but also reduce the administrative burdens that currently exist in tracking certifications and dive histories.

While certain challenges remain, such as data privacy concerns, accessibility in remote dive locations, and user adoption, ScubaChain aims to address these by prioritizing scalability, community engagement, and ease of use. With its emphasis on security and efficiency, ScubaChain is set to become an essential companion for divers everywhere, offering peace of mind and promoting a globally connected diving community where certifications are secure, dive experiences are easily trackable, and safety is at the forefront of each dive.



# **SOFTWARE REQUIREMENTS SPECIFICATION**

# **1. INTRODUCTION**

## **1.1. Purpose**

The ScubaChain project is a blockchain-based platform for scuba diving certification verification, and this article outlines its needs. To provide a reliable platform to the diving community, the project aims to create a decentralized, transparent, and safe system for confirming diving licenses.

Even through a smartphone application, the system will let divers confirm their credentials. IPFS (InterPlanetary File System) and blockchain technology will be used to guarantee that data is reliable and immutable.

## **1.2. Scope of Project**

In this project, we are creating ScubaChain, a revolutionary, blockchain-based platform to bring the scuba diving certification and dive log management ecosystem into the 21st century. Scuba Diving industry is still using the traditional systems based on the paper which are prone to loss, forgery, and limited accessibility. ScubaChain applies blockchain technology to offer a transparent, tamper-proof, and trustworthy digital solution to increase trust, data security, and user engagement among divers, dive masters, and dive centers.

The service will include two main parts: a web application and mobile application for dive centers, dive masters and divers. The web interface and the mobile app will let dive schools and dive masters issue and authenticate certificates, skills, and record dives on the blockchain. Meanwhile, they will allow divers to view and control their certifications and dive accounts, request validations, book dives and keep track of live updates such as dive maps and weather. They'll fix the current system and create a global, secure and standardized scuba diving ecosystem.

Certification management that is issuance and auditing of certifications in a permanently locked digital ledger and dive log management that helps divers keep their dive record digitally safe are its key features. Blockchain will be essential to ensure data authenticity and evasion of unauthorized modification or forgery. As it takes the place of traditional paper, certifications and dive records will be safer, more convenient and less prone to data loss with the new platform.

ScubaChain is tailored for 3 different user segments; divers, dive masters and dive centers. Diving customers will manage certifications, record dives, ask for verifications and join the community of diving users via social media and event participation on the mobile app. Certification verification, dive log checking, dive event management, and community events to be performed by dive masters. Dive centers will be administrative hubs that issue certifications

and keep a cloud of diver knowledge and experience. Each user persona will see customized screens and components for ease of use and for their specific purposes. In addition to basic certification and log management, ScubaChain incorporates several advanced features to enrich the user experience.

The platform will provide geolocation-based dive site maps, real-time weather and water condition updates, and interactive gamification elements. Divers will have the opportunity to earn NFT-based rewards for achieving milestones or participating in events, adding a gamified dimension to the platform that encourages engagement and fosters a sense of accomplishment. Social features, such as the ability to share dive experiences and achievements on social media, will further strengthen community connections.

The objectives will be attained by investing in cutting edge technology, incorporating blockchain for safety and reliability of data, building a web platform for dive centers and dive masters, and creating mobile applications for Android and iOS smartphones. Additional cloud-based services will provide other features, including integration of up-to-date weather forecasts and geolocation mapping. This technology-driven approach will provide the platform the desired user experience which is secure and dependable.

The main outputs of the project include web based interactive platform for dive centers and dive masters, mobile application for divers, and secure certification and log management blockchain structure. Other functionalities such as, milestone-based NFT rewards, interactive maps for dive sites, and tools to engage with the community will further enrich the usefulness of the platform. The scope however, does not rule out the management and integration of logs and certification as the main scope because certifying agencies and registration services might in future broaden the view.

Some elements fall outside the scope of this project at this time. For example, the introduction of hardware devices like underwater tablets for dive logging is not part of the focus. Advanced level training simulations or e-learning modules for certification courses in scuba diving also fall out of the scope of this project although they may be proposed in later versions. Integration with systems unrelated to blockchain certification is as well eliminated at this point.

In summary, ScubaChain wants to make paper work in the scuba diving industry a thing of the past by making online processes secure, transparent and community centered. The framework emphasized will develop towards incorporating advanced features and standards to build and manage global certification and dive logs, and strengthen the global diving community system.

### 1.3. Glossary

Term	Definition
<b>Blockchain</b>	A decentralized and immutable database system. Used in ScubaChain for securely verifying and storing diving licenses.
<b>Smart Contract</b>	Automated code pieces running on the blockchain. Manages processes such as NFT minting and license verification.
<b>IPFS (InterPlanetary File System)</b>	A decentralized file storage system. Securely stores diving licenses and NFT photographs.
<b>MetaMask</b>	An Ethereum-based digital wallet used for logging into the system and signing blockchain transactions.
<b>NFT (Non-Fungible Token)</b>	Unique digital assets. Converts photos taken during dives into digital collectibles recorded on the blockchain.
<b>Minting</b>	The process of creating new NFTs by recording digital content (e.g., photos, certificates) onto the blockchain through smart contracts.
<b>Diver</b>	A primary system user who queries and verifies their own diving license.
<b>Divemaster (Dive Center)</b>	A user type responsible for verifying divers' licenses and providing dive center information on the map.
<b>PADI/CMAS/SSI</b>	International organizations providing diving licenses. The system uses their databases for license verification.
<b>CID (Content Identifier)</b>	A hash value that uniquely identifies files stored on IPFS.
<b>Frontend</b>	The visual interface that users interact with.

<b>Backend</b>	The server-side system managing databases and API operations.
<b>API (Application Programming Interface)</b>	An interface facilitating data exchange between applications, such as querying diving licenses from the PADI/CMAS database.
<b>GPS (Global Positioning System)</b>	A system used for identifying the locations of dive centers on the world map.
<b>Pinning</b>	A mechanism used to ensure permanent storage of files on IPFS.
<b>Public Key</b>	Represents a user's identity on the blockchain. Used for license verification and login operations.
<b>Hash</b>	An algorithmic output that encrypts data uniquely on the blockchain, ensuring the accuracy of license information.
<b>JSON (JavaScript Object Notation)</b>	A lightweight and human-readable format used for data exchange in API calls and metadata files.
<b>WalletConnect</b>	A protocol enabling integration of digital wallets, like MetaMask, with mobile devices.
<b>Proof of Stake (PoS)</b>	A transaction validation mechanism for blockchain networks such as Ethereum, operating with low energy consumption.
<b>Authentication</b>	The process of securely logging users into the system, typically done via MetaMask wallet.
<b>Decentralization</b>	Refers to the operation of a system without reliance on a central authority, a key feature of blockchain and IPFS.

## 1.4. Overview of the Document

This document covers the ScubaChain project's technical and functional aspects, including how users will interact with the system and how it will operate. It's divided into two primary parts of the document, each aimed at a distinct user:

**General Overview and Product Viewpoint:** This part provides an overview of the main characteristics of the product, user profiles, and the technologies that "will be used" in its development.

**Requirement Specification:** Technical information on hardware and software interfaces, system performance standards, security standards, and interfaces with other systems is provided in this part.

## 2. OVERALL DESCRIPTION

### 2.1. Product Perspective

ScubaChain is a digital platform that aims to develop the diving industry. Diving certification, skill verification and diving records are transferred to the digital environment with Blockchain technology in a secure, transparent and unalterable way with advanced technology. With this life-making method, it streamlines all processes by strengthening the connections between individual divers, dive masters and dive centers. ScubaChain allows diving centers and dive leaders to verify certificates and record dives on the blockchain, allowing divers to easily check their personal records using the mobile application and instantly track their dive transactions and certificates. At the same time, whether divers are suitable for diving or not can be viewed through this application. ScubaChain aims to develop the diving industry by digitizing the registration processes and making diving easier and safer.

#### 2.1.1. Development Methodology

ScubaChain's development principle is based on agile, a software development philosophy that can respond quickly and easily to changing project requirements. This methodology specifically emphasizes collaboration, includes User-Centered Development processes, and receives continuous feedback, uses this feedback to improve the application, and enables rapid adjustments to the project.

The initial phase of the development process begins with determining the needs of divers, dive leaders and dive centers, and continues with a detailed analysis of what will be required by determining what the platform will be like, what its features will be, what work the platform will be used for. This analysis will form a basis to maximize the user experience and satisfaction of

the platform. Afterwards, the development team focuses on how the design of the platform will be and the functionality of the platform.

Agile methodology facilitates seamless communication and collaboration between divers, dive leaders and dive centers who will use the application. Thus, it enables the development team to detect potential problems in advance and intervene easily. At the same time, agile methodology ensures that the most up-to-date and best technologies are used in the project. This approach ensures that the application keeps up with future technologies and prevents any problems when updating it, and contributes to ScubaChain being a platform that complies with industry standards. During the development period, with the contribution of the iterative structure of the agile methodology, each component is quickly prototyped and then tested. Since this event will be held at regular intervals, it receives feedback from all kinds of users, ensuring that the product improves at every stage and creates a positive impact for users. This process aims to create a reliable, user-friendly and scalable platform while also making people love diving with ScubaChain.

## 2.2. User Characteristic

### 2.2.1. Divers

Divers form the primary user group of the platform. This group includes both beginner divers and experienced professionals. Their main needs are to manage diving certifications securely, log dives, and engage with the diving community. Additionally, community organizers and individuals planning diving events are included in this category. These users require:

- **Certification Management:** They need tools to verify existing diving certifications, upload new ones, and securely store them on the blockchain.
- **Dive Logging and Monitoring:** Divers want to record their past dives, manage details, and track equipment information using user-friendly tools.
- **Community Engagement:** Features like social media integration, NFT minting, and participation in competitions enhance their interaction with the community.
- **Mobile Application Usage:** A seamless and accessible mobile app experience for quick actions, sharing dive logs, and receiving reminders is essential.
- **Multilingual Support:** Supporting multiple languages is critical for the platform's global user base.

### 2.2.2 Divemaster

Dive masters represent the platform's second major user group. Their primary needs revolve around verifying divers' certifications, organizing dives, and simplifying their operational workflows.

- **Certification Verification:** They require a quick and reliable way to authenticate divers' certifications during training or events.
- **Dive Organization:** They need tools to manage divers' records, assign divemasters, and oversee event details efficiently.
- **Map and Location Management:** Dive masters need map-based tools to add new dive sites, update existing locations, and share these details with divers.
- **Blockchain Security:** Leveraging blockchain technology for reliable storage and verification of certifications is a key requirement.
- **Brand Profile Management:** Customizable profile pages to promote their services and showcase their offerings are highly valued.

## 3. REQUIREMENTS SPECIFICATION

### 3.1. External Interface Requirements

#### 3.1.1. User Interfaces

##### 1. Diver Interface

The interface for divers is designed to provide a seamless and engaging user experience while addressing their specific needs, as outlined in the user characteristics.

- **Mobile Application Dashboard:** The home screen of the mobile application offers a personalized dashboard. Divers can view their certification status, recent dive logs, notifications for upcoming certifications, and suggestions for dive sites based on their preferences.
- **Certification Management:** A dedicated section allows divers to upload and verify certifications using blockchain technology. The interface guides users step-by-step through the verification process and provides a clear status update on the certification's validity.
- **Dive Logbook:** An intuitive digital logbook enables divers to record dives, including details like location, depth, dive duration, and equipment used. The interface includes a timeline view to help users track their diving history visually.



- **NFT Minting for Dive Memories:** Divers can upload images or videos from their dives and mint them as NFTs directly from the app. This feature integrates seamlessly into the dashboard, ensuring an easy and quick minting process.
- **Social Integration:** The interface supports social sharing, allowing divers to post dive logs or achievements directly to platforms like Instagram or Twitter with one click.
- **Multilingual Support:** The user interface includes a language selection feature to accommodate a global user base, ensuring accessibility for non-English-speaking divers.

## 2. Dive Center and Divemaster

This interface caters to the operational needs of dive centers and divemasters, ensuring efficiency and accuracy.

- **Certification Verification Panel:** The interface provides a streamlined tool for verifying divers' certifications by scanning QR codes or entering blockchain-based certification IDs.
- **Event and Dive Management:** A calendar-based interface allows dive centers to schedule dives, assign divemasters, and manage participant details efficiently.
- **Location and Map Tools:** Dive centers can add or update dive site information through an integrated map tool. Users can pin dive locations, add descriptions, and upload images to create a comprehensive dive map.
- **Profile Management:** Dive centers can customize their profiles by adding branding elements, services offered, and promotional content. This profile is visible to divers when they search for dive centers.
- **Blockchain Interaction:** Tools for securely uploading and managing certification data using blockchain technology are integrated into the interface. The system ensures that all interactions are intuitive and do not require advanced technical knowledge.
- **Analytics Dashboard:** Dive centers can view analytics related to their operations, such as the number of certifications verified, participants per event, and feedback from divers.

### 3. Common Features

Both divers and divemasters share access to certain common functionalities designed to enhance user experience.

- **Login and Authentication:** Secure login via MetaMask or WalletConnect ensures data privacy. The authentication process is simple and user-friendly, allowing quick access for all users.
- **Notifications and Reminders:** The notification center alerts users about expiring certifications, upcoming dives, or new features added to the platform.
- **Help and Support:** An integrated support system provides FAQ sections to assist users with technical or operational issues.
- **Mobile-First Design:** Both interfaces are optimized for mobile devices, ensuring responsive and visually appealing layouts for smartphones and tablets.

#### 3.1.2. Hardware Interfaces

To access this platform, the necessary hardware features are up-to-date, tablets, laptops and desktop computers that can access any website, as well as smart devices such as any phone or tablet that can download current applications from its own store application.

#### 3.1.3. Software Interfaces

The software interfaces for the ScubaChain project will be as follows:

##### • Mobile Application (Front-end):

1. It will be developed using Flutter.
2. It will provide separate interfaces for divers and dive centers.
3. License validation, viewing blockchain hashes and IPFS connections features will be added.

##### • Server (Back-end):

1. It will be developed using Node.js (Express.js).
2. PostgreSQL will be used to manage user and license data.
3. RESTful APIs will handle communication between the front-end and back-end and will perform validation with PADI/CMAS databases.

- **Blockchain and IPFS Integration:**

1. The Ethereum blockchain will be used to validate license data through smart contracts written in Solidity.
2. License documents will be stored on IPFS, which ensures decentralized storage by providing access via Content Identifier (CID).

### **3.1.4 Communication Interfaces**

Even though this application works on two different device / platform types, its general functional structure is the same. However, examining these platforms under two separate headings will highlight which tools are required for each device type. To deal with blockchain integration, all systems will be developed in Solidity, which is a programming language used for the Ethereum blockchain platform.

#### **3.1.4.a Web-Based Platform**

General user types in this Project are divers and dive masters. They would use these functionalities that:

1. Verification of certifications and recording dive logs
2. Issuing new certifications digitally and storing objects
3. User management and access control.

As it is mentioned in literature review, classical Web 2.0 tools (HTML, CSS) and Web 3.0 technologies (React.js, Node.js, Express.js) are enough for developing web platform of this project. Access control issue is solved via HTTPS, user authentication protocols (OAuth or digital signatures) for now.

#### **3.1.4.b Mobile Platform**

With the same user profiles mentioned in 3.1.4.a Web-based Platform, it's just enough for determining which tools will be used. Flutter for cross-platform support, NFC and QR-Code technology for basic verifications. Then, the mobile app connects to the blockchain database via APIs to fetch and send real-time data.

### **3.1.4.c API Integrations & Security Layer**

Third parties, such that government databases, weather services, and social media platforms, will be used for API integrations. The usage purposes are verifying/requesting certifications through government or official databases and integrating real-time weather and geolocation data. Data transfer formats are in JSON/XML formats.

For security and encryption layer, this application's system have to protecting user data and digital identities through encryption (SSL/TLS) and ensuring data integrity with digital signatures. It can be provided with using OpenZeppelin, it mentioned in detail in literature review.

## **3.2. Functional Requirements**

### **Use Cases:**

- Register/Login with Metamask
- Installing the License
- Log a Dive Information Logout
- Mint on NFT Photos Token While Diving
- Searching Dive Centers
- View License
- Editing Profile
- Login to the System
- Creating/Joining a Crew & Event
- Verify Diver Certification
- View Diver Logs
- Manage Dive Events
- Add or Update Dive Locations on Map

**Diagram:**



## 1. Register/Login with Metamask

<b>Use Case Number</b>	Use Case 1
<b>Use Case Name</b>	Register/Login with Metamask
<b>Actor</b>	Diver
<b>Description</b>	The diver registers or logs into the system using their Metamask wallet.
<b>Precondition</b>	Diver has a Metamask wallet installed.
<b>Scenario</b>	1. Diver selects Metamask login. 2. Diver connects wallet and verifies identity. 3. System grants access.
<b>Postcondition</b>	Diver successfully registers or logs in via Metamask.
<b>Exceptions</b>	Wallet connection failure, authentication error.

## 2. Installing the License

<b>Use Case Number</b>	Use Case 2
<b>Use Case Name</b>	Installing the License
<b>Actor</b>	Diver
<b>Description</b>	The diver enters their SSN (Social Security Number) to upload the license to the system. The system verifies the license with PADI or CMAS. If successful, the license is confirmed, and its hash is stored on the Blockchain.
<b>Precondition</b>	Diver has a valid license.
<b>Scenario</b>	1. Diver enters SSN and license details. 2. The system verifies the license with PADI/CMAS. 3. License is validated and stored on Blockchain.
<b>Postcondition</b>	Diver's license is verified and added to the system.
<b>Exceptions</b>	Invalid SSN or license details, system verification failure.

### 3. Log a Dive Information

<b>Use Case Number</b>	Use Case 3
<b>Use Case Name</b>	Log a Dive Information
<b>Actor</b>	Diver
<b>Description</b>	The diver logs dive details (e.g., location, duration, depth) into the system. The data is stored securely on Blockchain.
<b>Precondition</b>	Diver is logged into the system.
<b>Scenario</b>	1. Diver enters dive details. 2. System saves the data to Blockchain.
<b>Postcondition</b>	Dive information is securely stored in the system.
<b>Exceptions</b>	Invalid data input, Blockchain connectivity issues.

### 4. Mint on NFT Photos Token While Diving

<b>Use Case Number</b>	Use Case 4
<b>Use Case Name</b>	Mint on NFT Photos Token While Diving
<b>Actor</b>	Diver
<b>Description</b>	The diver uploads photos taken during the dive. The system converts them to NFTs, stores their CID on Blockchain, and the image on IPFS.
<b>Precondition</b>	Diver is logged into the system with access to IPFS.
<b>Scenario</b>	1. Diver uploads photos. 2. System converts photos to NFT. 3. CID is stored on Blockchain and file on IPFS.
<b>Postcondition</b>	Photos are successfully minted as NFTs.
<b>Exceptions</b>	Photo upload failure, Blockchain or IPFS connectivity issues.

## 5. Searching Dive Centers

<b>Use Case Number</b>	Use Case 5
<b>Use Case Name</b>	Searching Dive Centers
<b>Actor</b>	Diver
<b>Description</b>	The diver searches for nearby or specific region dive centers on a map and views their details.
<b>Precondition</b>	System access with map integration.
<b>Scenario</b>	1. Diver searches for dive centers. 2. System displays relevant centers and their details.
<b>Postcondition</b>	Diver can access information about desired dive centers.
<b>Exceptions</b>	No results found, system or map integration issues.

## 6. View License

<b>Use Case Number</b>	Use Case 6
<b>Use Case Name</b>	View License
<b>Actor</b>	Diver
<b>Description</b>	The diver can view their uploaded license through a visual interface.
<b>Precondition</b>	License information is already uploaded and stored on Blockchain.
<b>Scenario</b>	1. Diver selects the option to view their license. 2. System retrieves and displays license details.
<b>Postcondition</b>	Diver successfully views their license details.
<b>Exceptions</b>	License not found, Blockchain retrieval failure.



## 7. Editing Profile

<b>Use Case Number</b>	Use Case 7
<b>Use Case Name</b>	Editing Profile
<b>Actor</b>	Diver
<b>Description</b>	The diver updates personal profile information such as name, surname, and contact details.
<b>Precondition</b>	Diver is logged into the system.
<b>Scenario</b>	1. Diver selects the option to edit their profile. 2. Diver updates profile details. 3. System saves the changes.
<b>Postcondition</b>	Profile information is successfully updated.
<b>Exceptions</b>	Invalid input, system update failure.

## 8. Login to the System

<b>Use Case Number</b>	Use Case 8
<b>Use Case Name</b>	Login to the System
<b>Actor</b>	Diver
<b>Description</b>	The diver logs into the system to access their personal account.
<b>Precondition</b>	Diver has valid login credentials.
<b>Scenario</b>	1. Diver enters username and password. 2. System verifies credentials. 3. Diver accesses their account.
<b>Postcondition</b>	Diver successfully logs into the system.
<b>Exceptions</b>	Incorrect credentials, system login failure.

## 9. Creating/Joining a Crew & Event

<b>Use Case Number</b>	Use Case 9
<b>Use Case Name</b>	Creating/Joining a Crew & Event
<b>Actor</b>	Diver
<b>Description</b>	The diver creates or joins a crew or a diving event through the system.
<b>Precondition</b>	Diver is logged into the system.
<b>Scenario</b>	1. Diver creates or searches for an event. 2. System displays event details. 3. Diver joins or creates an event.
<b>Postcondition</b>	Diver successfully joins or creates an event.
<b>Exceptions</b>	Event creation failure, joining restrictions.

## 10. Verify Diver Certification

<b>Use Case Number</b>	Use Case 10
<b>Use Case Name</b>	Verify Diver Certification
<b>Actor</b>	Dive Center/DiveMaster
<b>Description</b>	The dive center or instructor verifies the diver's certification through organizations like PADI or CMAS.
<b>Precondition</b>	Diver certification details are available.
<b>Scenario</b>	1. Dive center initiates certification verification. 2. System contacts PADI/CMAS for verification. 3. Certification is validated.
<b>Postcondition</b>	Diver's certification is successfully verified.
<b>Exceptions</b>	Verification failure, invalid certification.

## 11.View Diver Logs

<b>Use Case Number</b>	Use Case 11
<b>Use Case Name</b>	View Diver Logs
<b>Actor</b>	Dive Center/DiveMaster
<b>Description</b>	The dive center or instructor views the diver's logged dive records.
<b>Precondition</b>	Dive records are stored on Blockchain.
<b>Scenario</b>	1. Dive center requests diver logs. 2. System retrieves logs from Blockchain. 3. Logs are displayed.
<b>Postcondition</b>	Dive center successfully views the diver's logs.
<b>Exceptions</b>	Log retrieval failure, Blockchain connectivity issues.

## 12.Manage Dive Events

<b>Use Case Number</b>	Use Case 12
<b>Use Case Name</b>	Manage Dive Events
<b>Actor</b>	Dive Center/DiveMaster
<b>Description</b>	The dive center or instructor manages diving events, including creating, editing, or canceling events.
<b>Precondition</b>	Access to event management system.
<b>Scenario</b>	1. Dive center creates or edits event details. 2. System saves or updates event information. 3. Event is published or updated.
<b>Postcondition</b>	Diving events are successfully managed.
<b>Exceptions</b>	Event creation or update failure, system access issues.

### 13.Add or Update Dive Locations on Map

<b>Use Case Number</b>	Use Case 13
<b>Use Case Name</b>	Add or Update Dive Locations on Map
<b>Actor</b>	Dive Center/DiveMaster
<b>Description</b>	The dive center or instructor adds or updates dive locations on a map.
<b>Precondition</b>	Access to map and location management system.
<b>Scenario</b>	1. Dive center adds or updates a location. 2. System saves location details. 3. Map is updated with new location.
<b>Postcondition</b>	Dive locations are successfully updated on the map.
<b>Exceptions</b>	Location addition failure, map integration issues.

### 3.3 Performance Requirements

The performance requirements for ScubaChain focus on ensuring the system operates efficiently and reliably. The platform should provide low-latency responses for basic user functionalities but it would have one hour tolerance for certification verifications and dive log updates. Generally, it should handle increasing user numbers, limited requests' size per user and transaction volumes without degradation in overall performance. Also, with minimum corruption rate, the system should storage and save the all data with zero incidents of any unauthorized modification. The system should offer a smooth and fast user interface for both web and mobile applications.

About the issue, efficiency & total cost, the system should provide to optimize energy consumption and total fee, especially for operations involving blockchain consensus mechanisms and blockchain transactions/storage operations. There is no expected desirement level for transaction throughput, latency, availability and fault tolerance for now, due to uncertainty of development stage.

## **3.4 Software System Attributes**

### **3.4.1 Portability**

The system's mobile application should support both IOS and Android platforms and updated versions using a single codebase (like Flutter) and web platform should be compatible with major browsers (Chrome, Firefox, Safari, Edge etc.). Also, the blockchain integration must support different blockchain platforms (Ethereum) to adapt to user preferences or future technological shifts.

### **3.4.2 Scalability**

For scalability of this project, off-chain storage solutions like IPFS for large data files (e.g., dive logs, certificates) to reduce on-chain congestion. Elastic cloud infrastructure (like Amazon Cloud Services) also would be used for the web platform to manage high user loads and user requests.

### **3.4.3 Adaptability**

Possible requirements are constructing modular architecture using APIs and microservices to easily incorporate new features (e.g., additional certification bodies, blockchain elements like NFTs) and support for smart contract upgrades to address evolving certification standards or regulations.

### **3.4.4 Usability**

The main issue in this case, determining which users can interact with the system. Intuitive user interfaces for both web and mobile platforms, designed with divers, dive centers, and instructors in mind. In future, also multilingual support can be added for the international diving community.

### **3.4.5 Performance**

Although there is no expectation about performance desirability criteria, the general mission is receiving low-latency blockchain transactions, high throughput for certification and dive log updates and minimal downtime with a target of high and stable availability.

### 3.5. Safety Requirement

#### 1. Blockchain Ensures Immutable Data Storage

<b>Name</b>	<b>Blockchain Ensures Immutable Data Storage</b>
<b>Purpose/Description</b>	Enhance security by ensuring data is stored immutably on the blockchain.
<b>Inputs</b>	User-provided data (e.g., license information, NFT data).
<b>Process</b>	Data is recorded on the blockchain and becomes immutable. All transactions are verified with digital signatures.
<b>Output</b>	Data is securely stored on the blockchain and can be tracked with public logs.

#### 2. Secure Transactions with Encryption and Digital Signatures

<b>Name</b>	<b>Secure Transactions with Encryption and Digital Signatures</b>
<b>Purpose/Description</b>	Ensure secure data transmission and transaction verification using encryption and digital signatures.
<b>Inputs</b>	User's digital signature, transaction data.
<b>Process</b>	All data transfers are encrypted and digital signatures verified. Unauthorized access is prevented.
<b>Output</b>	Transactions are securely executed, and user data is protected.

### 3. Access Control Mechanisms and Unauthorized Access Prevention

<b>Name</b>	<b>Access Control Mechanisms and Unauthorized Access Prevention</b>
<b>Purpose/Description</b>	Provide access control mechanisms to protect user data and prevent unauthorized access.
<b>Inputs</b>	User session information (e.g., authentication tokens, user roles).
<b>Process</b>	Authorize logged-in users. Unauthorized access attempts are blocked, and incidents are logged.
<b>Output</b>	Only authorized users access data, and the system is protected from unauthorized entries.

### 4. Public Logs for All Blockchain Transactions

<b>Name</b>	<b>Public Logs for All Blockchain Transactions</b>
<b>Purpose/Description</b>	Ensure transparency by storing all transactions in publicly accessible logs.
<b>Inputs</b>	Blockchain transaction data (e.g., transaction ID, date, user address, transaction details).
<b>Process</b>	Each transaction is recorded as a log and made publicly accessible. These logs are stored on the blockchain.
<b>Output</b>	Transactions are transparently tracked and auditable.

# **SOFTWARE DESIGN DESCRIPTION**



# **1. INTRODUCTION**

## **1.1 Purpose**

The ScubaChain project seeks to revolutionize scuba diving certification verification by leveraging blockchain technology to create a reliable, decentralized, and transparent platform for managing diving credentials. The platform aims to eliminate issues associated with traditional paper-based systems, such as forgery and limited accessibility, by providing a secure and immutable digital ledger.

Through an integrated smartphone application, divers will have the ability to effortlessly confirm their certifications, ensuring ease of use and reliability. The system incorporates cutting-edge technologies such as the Interplanetary File System (IPFS) for decentralized storage and blockchain for data authenticity, enabling a seamless, tamper-proof solution tailored for the global diving community.

## **1.2 Scope**

In this Software Design Document (SDD), we outline ScubaChain, a platform designed to revolutionize the scuba diving industry by transitioning from traditional paper-based systems to a secure, blockchain-based digital ecosystem. ScubaChain provides a transparent, tamper-proof solution for managing certifications and dive logs, ensuring data security, accessibility, and user engagement for divers, dive masters, and dive centers.

The platform consists of a web application for dive centers and dive masters and a mobile application for divers. These tools enable users to issue and verify certifications, log dives, and access real-time updates such as dive maps and weather conditions. Advanced features, including geolocation-based dive site maps, milestone based NFT rewards, and social sharing capabilities, enrich the user experience while fostering a global diving community.

By leveraging blockchain technology, ScubaChain ensures data authenticity and prevents unauthorized modifications or forgery. This approach not only enhances trust and reliability but also paves the way for a standardized and globally accessible scuba diving ecosystem. With future scalability in mind, ScubaChain is set to transform how the diving industry manages its critical processes, making them more secure, efficient, and community-driven.

## 1.3 Glossary

Term	Definition
Dive Center	A user entity responsible for verifying diver certifications, managing events, and updating dive locations.
Dive Master	A user entity with responsibilities such as managing dive events, verifying certifications, and assisting divers.
Diver	A primary user of the system, responsible for managing their diving certifications and participating in events.
License Hash	A unique identifier generated through blockchain technology to securely verify and store diving certifications.
Transaction_ID	An identifier for transactions logged in the blockchain to track operations like certification or NFT minting.
Smart Contract	Blockchain-based automated scripts that execute specific tasks like hashing licenses, NFTs, and dive logs.
System Information	The central module handling system-level operations such as user authorization, profile updates, and data requests.

## 1.4 Overview of Document

The Software Design Document (SDD) for the ScubaChain project outlines the architectural and design details essential for implementing a blockchain-based solution in the scuba diving industry. This document serves as a bridge between the requirements specified in the Software Requirement Specification (SRS) document and the actual development process by providing a detailed blueprint of the system's structure and components. The SDD for the

ScubaChain is structured to ensure a comprehensive understanding of the system's design, covering key aspects such as system architecture, data flow, and interaction patterns. This document is aimed at developers, project stakeholders, and anyone involved in the software development lifecycle, ensuring clarity and alignment across all phases of the project. The key objectives of this document include providing a clear understanding of the system's purpose and problem domain by highlighting the challenges in the scuba diving industry and how blockchain technology addresses them; defining the scope of the design by establishing the boundaries of the system and detailing the primary functionalities; describing the system architecture and its components by illustrating the high-level structure through diagrams and technical descriptions; specifying the technologies and methodologies used by identifying tools, frameworks, and best practices essential for the system's implementation; and ensuring traceability between requirements and design by linking the design elements to the specific requirements outlined in the SRS document. By presenting a well-structured and detailed design framework, this document aims to facilitate the development of a robust, scalable, and secure blockchain system tailored to the needs of the scuba diving community. Each section of this document delves into specific aspects of the system, ensuring a holistic and methodical approach to design and implementation.

## **1.5 Motivation**

This motivation section provides a comprehensive explanation of the origins of ScubaChain, its objectives, and its intended achievements. ScubaChain was developed with the aim of modernizing the scuba diving industry, which currently relies on fragile paper-based systems for managing certifications and dive logs. By leveraging blockchain technology, ScubaChain offers a secure, transparent, and tamper-resistant digital platform that enhances both integrity and accessibility. Additionally, ScubaChain seeks to support a sustainable diving ecosystem by integrating advanced features such as real-time dive area information and service location maps. Although ScubaChain was initially launched as a local application, our primary goal is to facilitate its adoption on a global scale.

## **2. SYSTEM DESIGN**

The ScubaChain project leverages blockchain technology to provide a secure, transparent, and decentralized platform for scuba diving license verification. The system is designed to address existing inefficiencies and security risks in traditional license management processes by introducing a modern, user-centric digital solution. This document outlines the architectural design, functional components, explanation diagrams, and interaction flow that collectively define the ScubaChain system.

### **2.1 Architectural Design**

This project includes totally six layer, consists of blockchain layer, smart contract layer, IPFS & database layer, backend layer, frontend layer and authentication & identity management layer. Blockchain serves as the backbone for secure issue and relates the objects with decentralized data storage (Which is IPFS component). This layer implements a public or permissioned blockchain (e.g., Ethereum) for managing license data records and verification transactions.

Smart contract layer automates license verification, renewal, and level-up processes based on predefined rules. In addition, it allows us to use functions (Minting, OpenSea publishing etc.) related to NFT items.

The IPFS & Database layer are divided into three separate parts. IPFS part handles the images about to converted into NFT and normal images. Blockchain sends to the PostgreSQL system and database handles the storage of dive logs and special hashes. General PostgreSQL Database stores the normal data types such as user credentials, location information, rating etc.

Backend layer manages the API & user requests; determines which user has access to which functions and processes API requests from other applications in the background. It determines at which layer the called functions will be processed and what outputs they will give to the user after processing.

The frontend & identity management layer indicates the application differently for each different user type, changes the appearance of the application and allowed functions. Also, this the identity management layer that it allows to sign up with Metamask account.

## 2.1.1 Problem Description

The ScubaChain project addresses critical issues within the scuba diving industry, which currently relies on outdated, paper-based systems for certification management and dive logging. These traditional methods are prone to loss, forgery, inefficiencies, and accessibility challenges, leading to a lack of trust and reliability. Divers face difficulties verifying their credentials, while dive centers struggle with secure data management and fraud prevention. The fragmented nature of the existing ecosystem further complicates collaboration among divers, dive masters, and organizations. ScubaChain aims to revolutionize this ecosystem by integrating blockchain technology to ensure transparency, security, and immutability. The platform will provide decentralized certification verification, enabling divers to manage their credentials seamlessly through mobile and web applications. Additionally, it facilitates digital dive logging, reducing dependency on physical records. By incorporating real-time data such as weather updates, geolocation-based dive site mapping, and gamified NFT rewards, the system enhances user engagement and fosters a connected diving community. Ultimately, ScubaChain seeks to establish a global, standardized, and secure digital framework, addressing current inefficiencies while paving the way for a more collaborative, trustworthy, and innovative scuba diving industry.

## 2.1.2 Technologies Used

The ScubaChain project incorporates a combination of advanced technologies to ensure security, scalability, and usability for now & future. Each technology is selected based on its ability to address the specific requirements of the system with most stable ones, including blockchain integration, decentralized identity management, and user-friendly interfaces. Below is a detailed breakdown of the technologies used:

### 1. Blockchain Technology

**Ethereum:** Ethereum (public blockchain) is considered for their robust smart contract capabilities, security features, and widespread adoption. Ethereum enables public, decentralized verification, uses Proof of Stake (PoS) for consensus mechanism. [17]

**Smart Contracts:** Written in Solidity (for Ethereum), smart contracts automate certification issuance, verification, and updates. Ensures immutable and tamper-proof record keeping. [18]

## 2. Frontend Development

**Web Application:** Built using **React.js** for its component-based architecture, responsiveness, and scalability. Provides an intuitive interface for dive centers and certification organizations to validate licenses and manage certifications.

**Mobile Application:** Developed using **Flutter** for cross-platform compatibility, ensuring a seamless experience on both Android and iOS devices. Enables divers to access their certifications, manage dive logs, and interact with the system easily. [19]

## 3. Backend Development

**Node.js:** Used to build a robust, scalable backend server to handle API requests, manage business logic, and facilitate blockchain interactions. [20]

**Express.js:** A lightweight web application framework for Node.js, streamlining the development of RESTful APIs.

## 4. Database Management

**PostgreSQL:** A relational database system used for storing off-chain data, such as user profiles and certification metadata. Offers strong consistency, scalability, and integration capabilities with blockchain-based applications. [21]

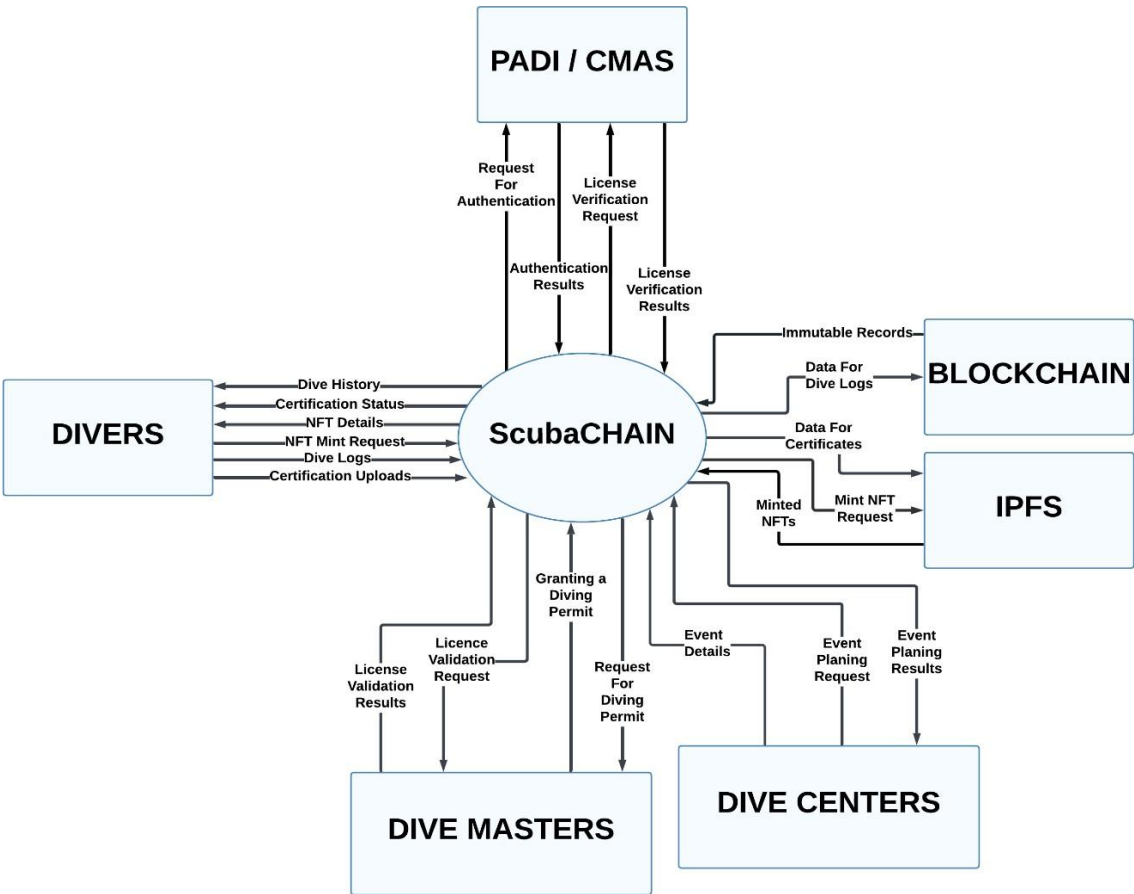
**IPFS (InterPlanetary File System):** Used for decentralized storage of certification-related documents, ensuring data integrity and accessibility. [22]

## 5. Authentication and Identity Management

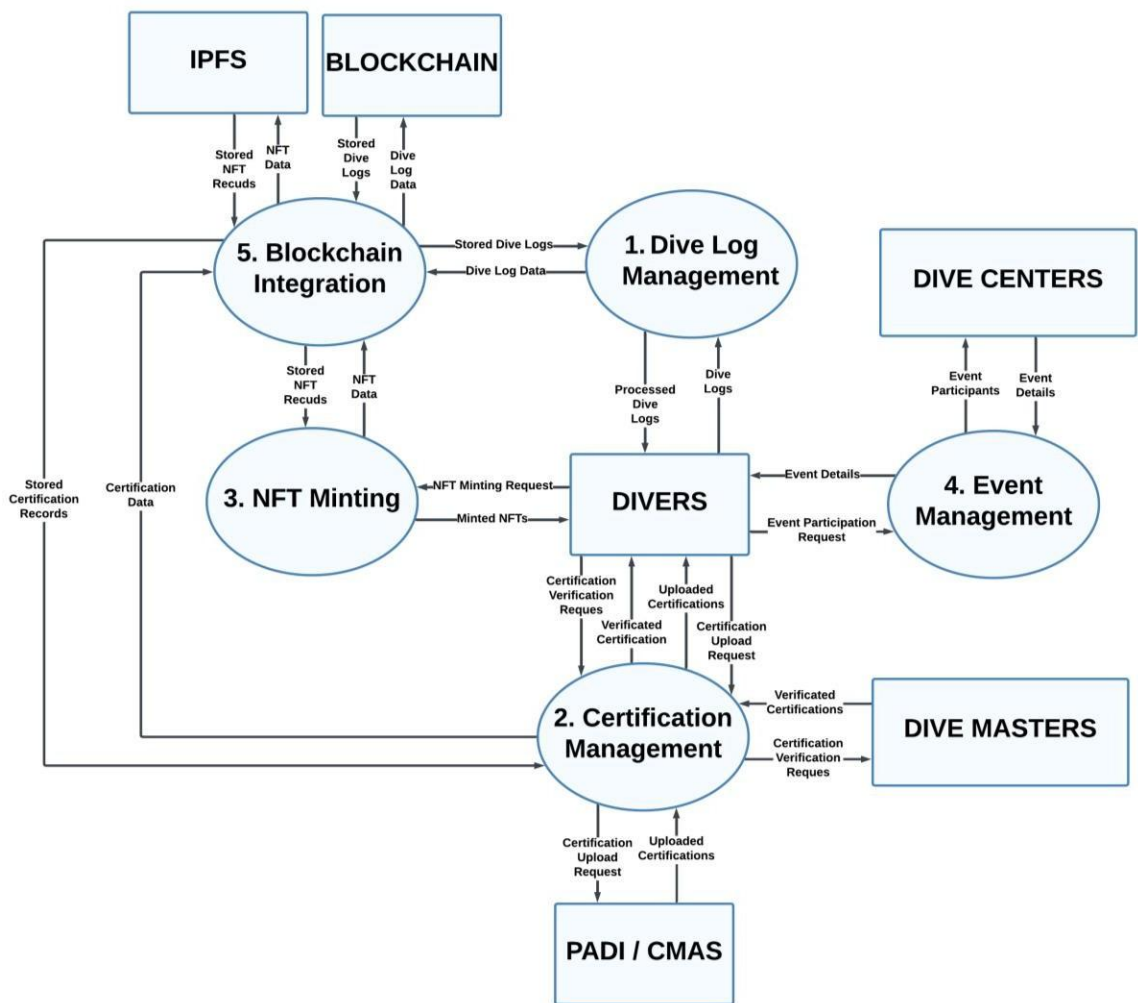
**Digital Wallet Integration:** Supports blockchain wallets like **MetaMask** for secure user authentication and interaction with the blockchain. [23]

# 2.1.3 Data Flow Diagram (DFD)

## Level 0 (Context Diagram)

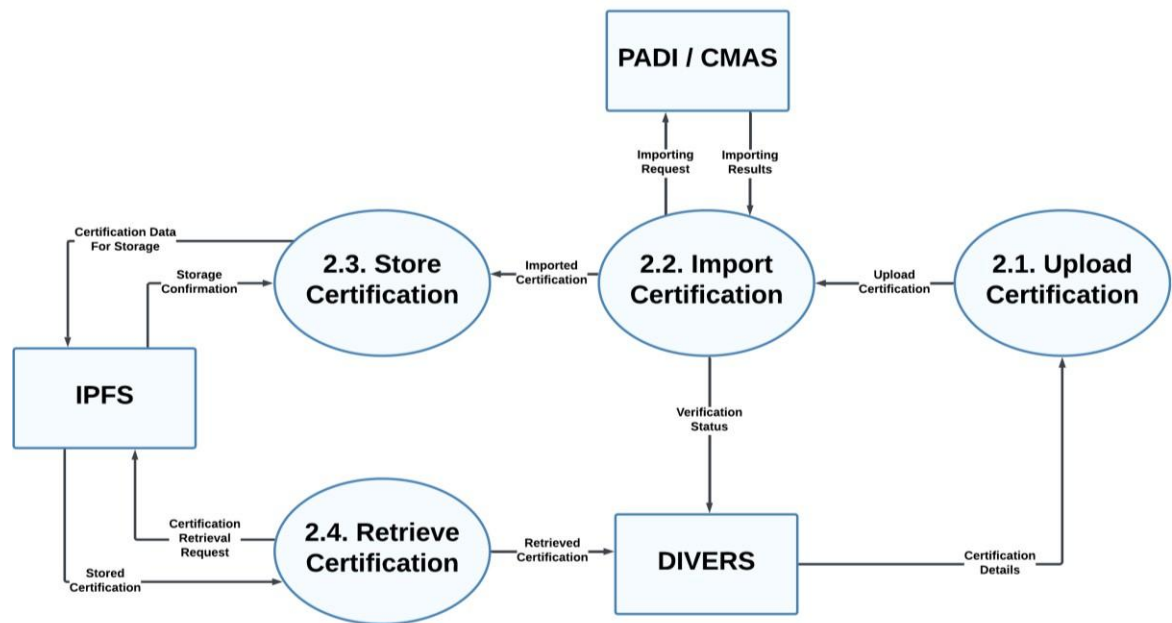


Level 1

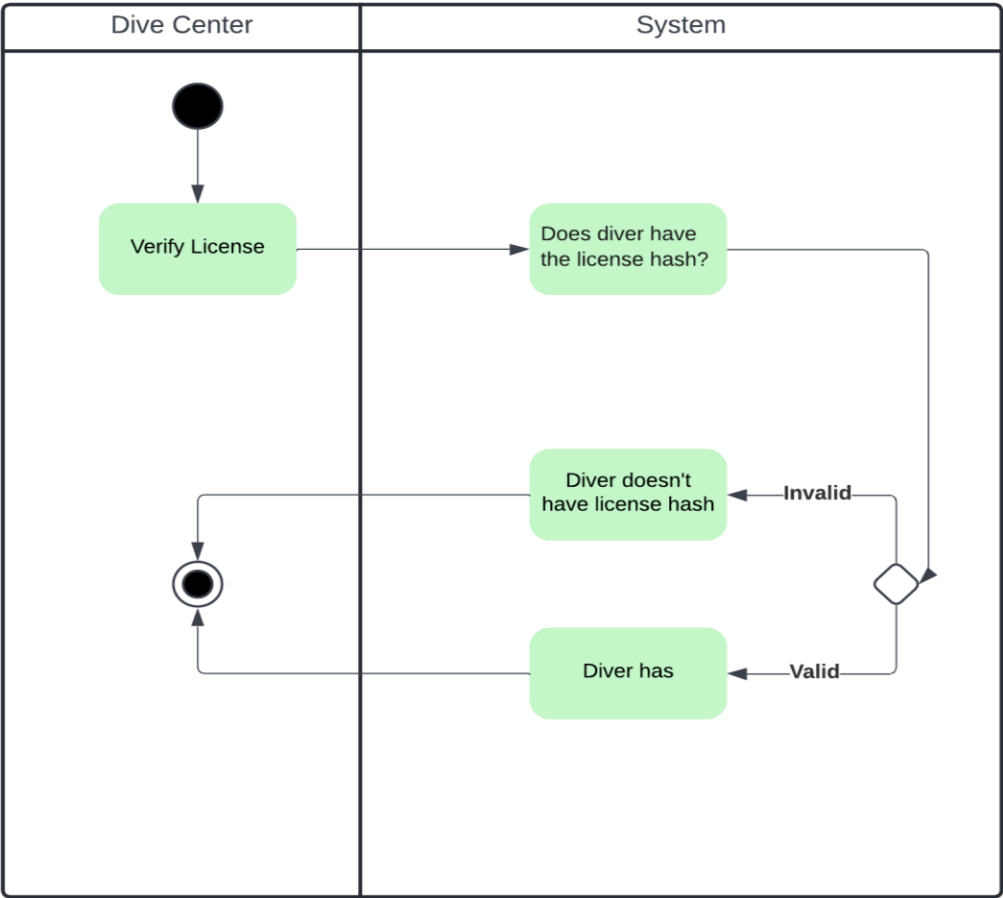




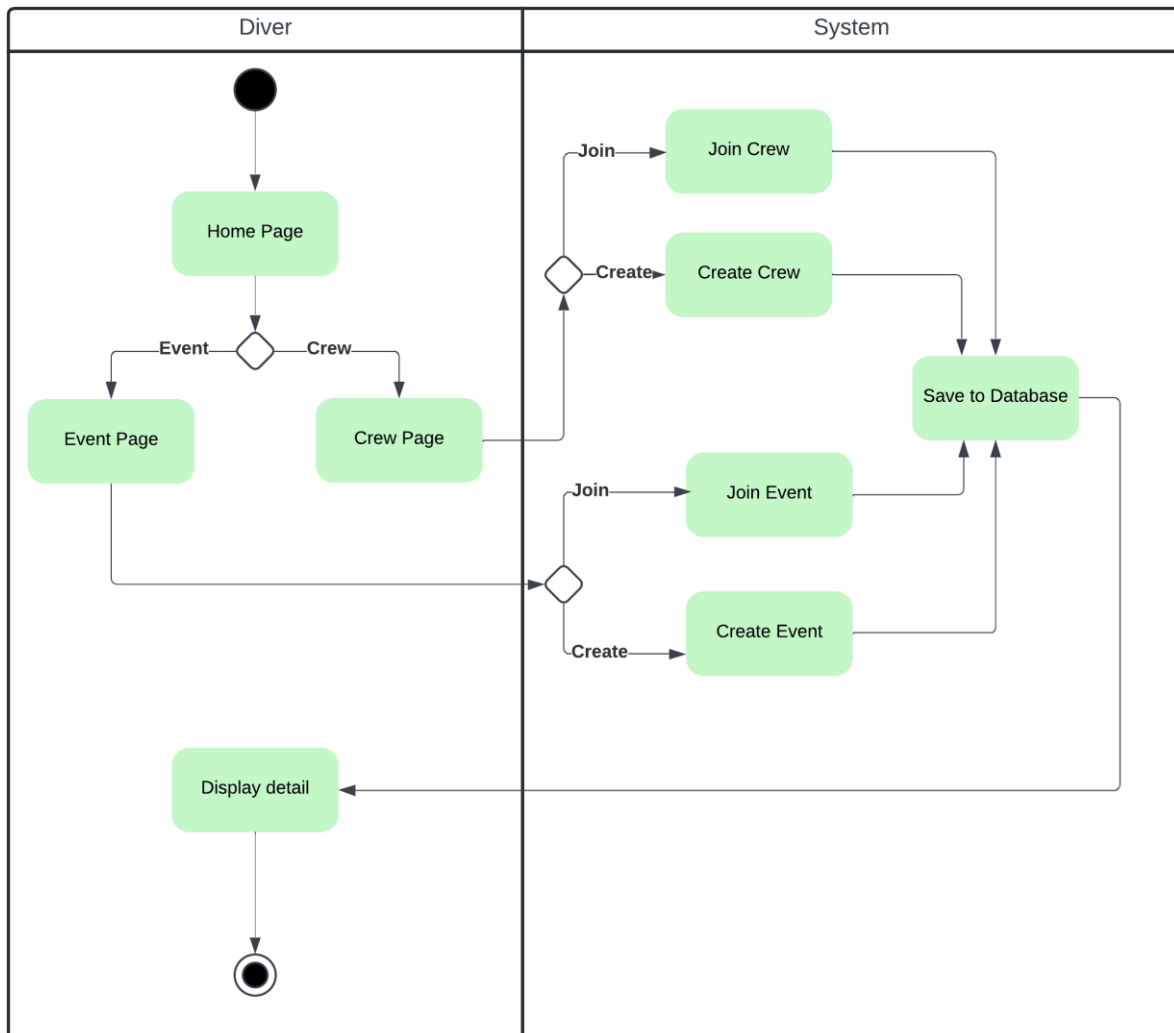
Level 2



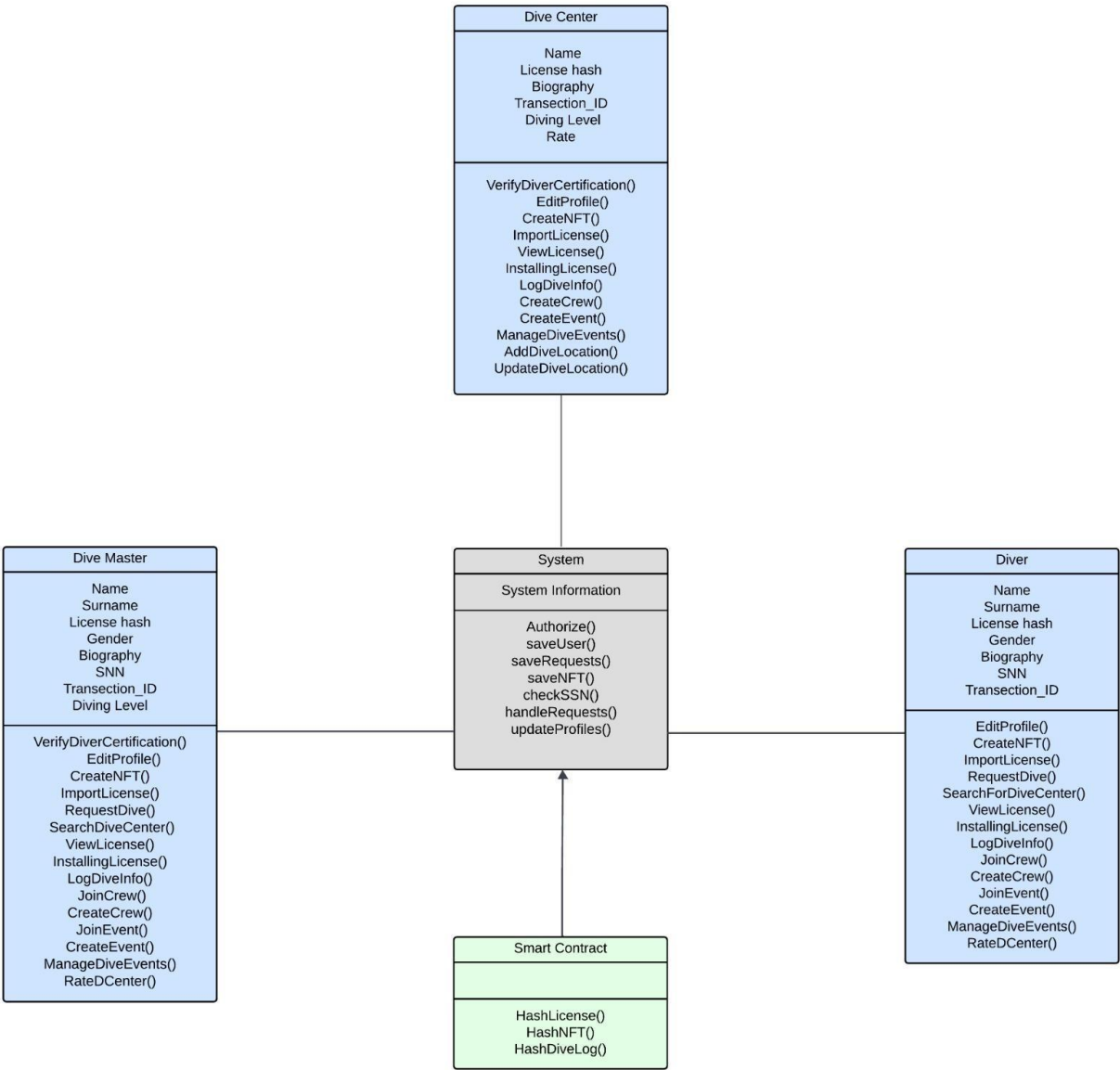
2.1.4 Activity Diagram





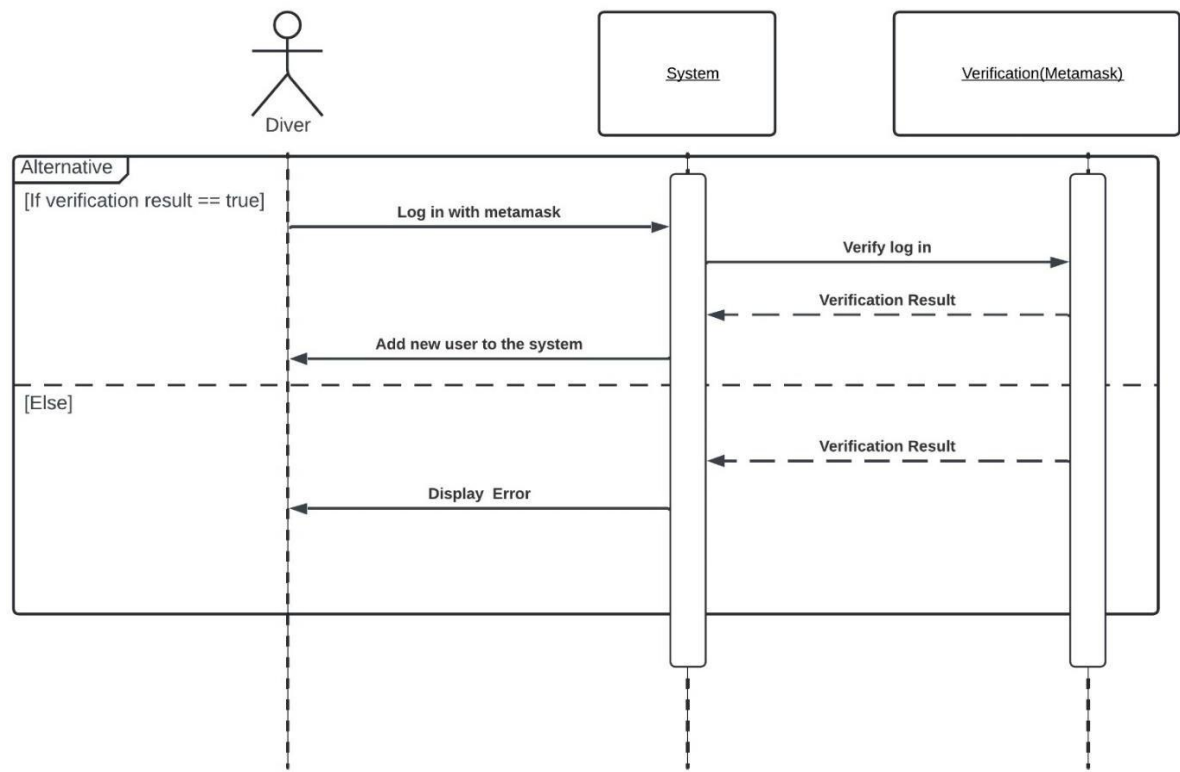


# 2.1.5 Class Diagram

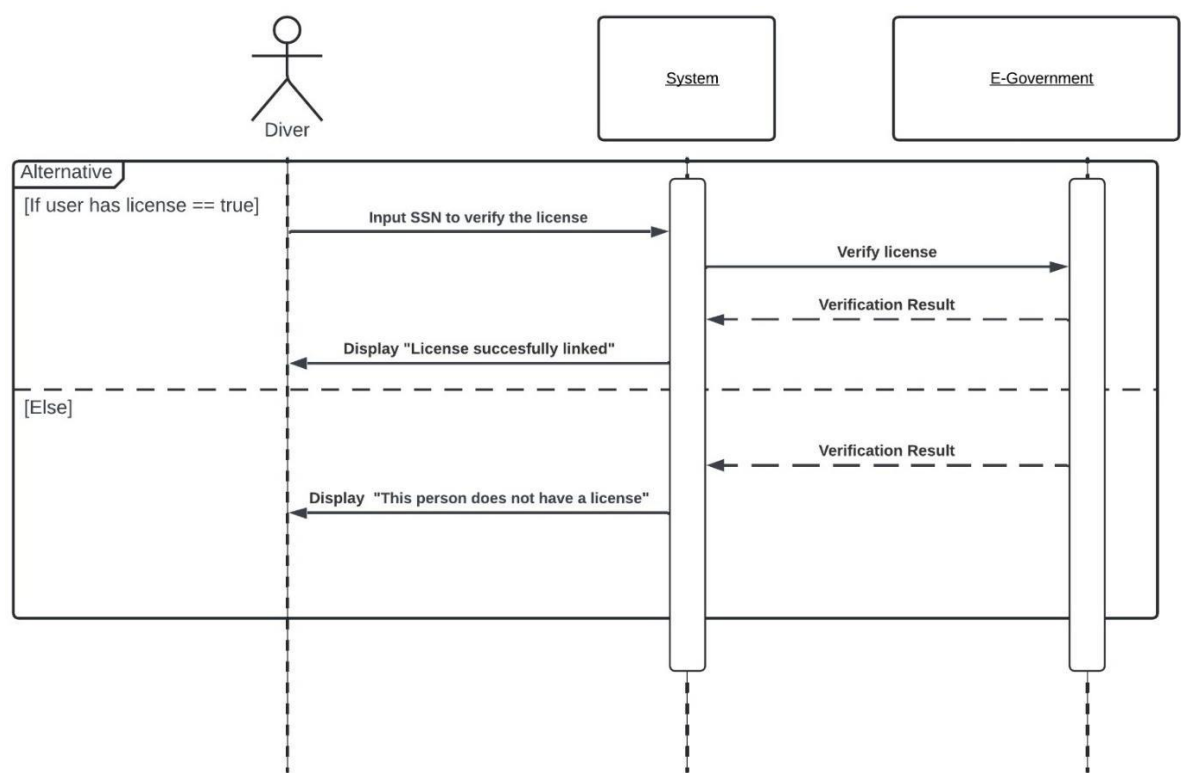


# 2.1.6 Sequence Diagram

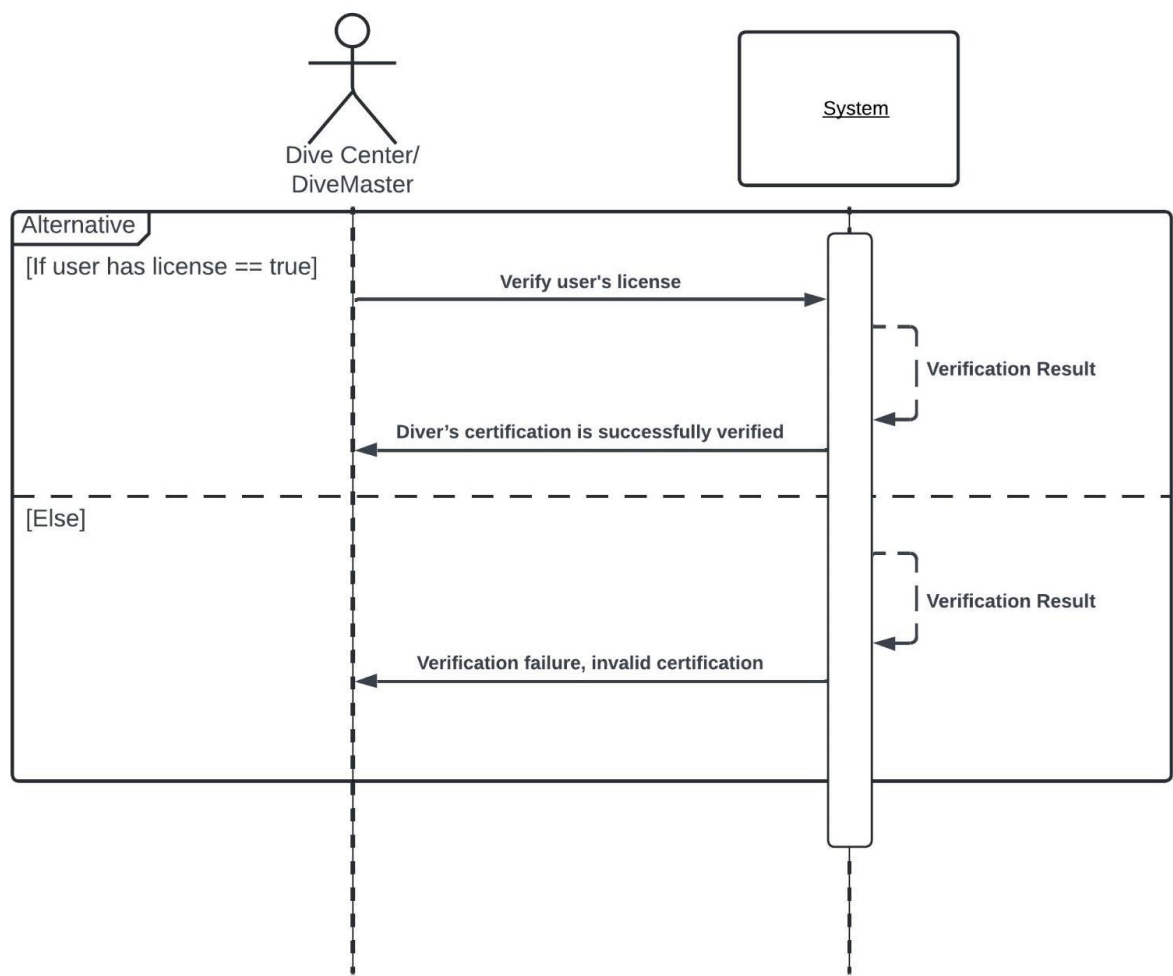
Sequence Diagram of Use Case 1 - Register/Login with Metamask



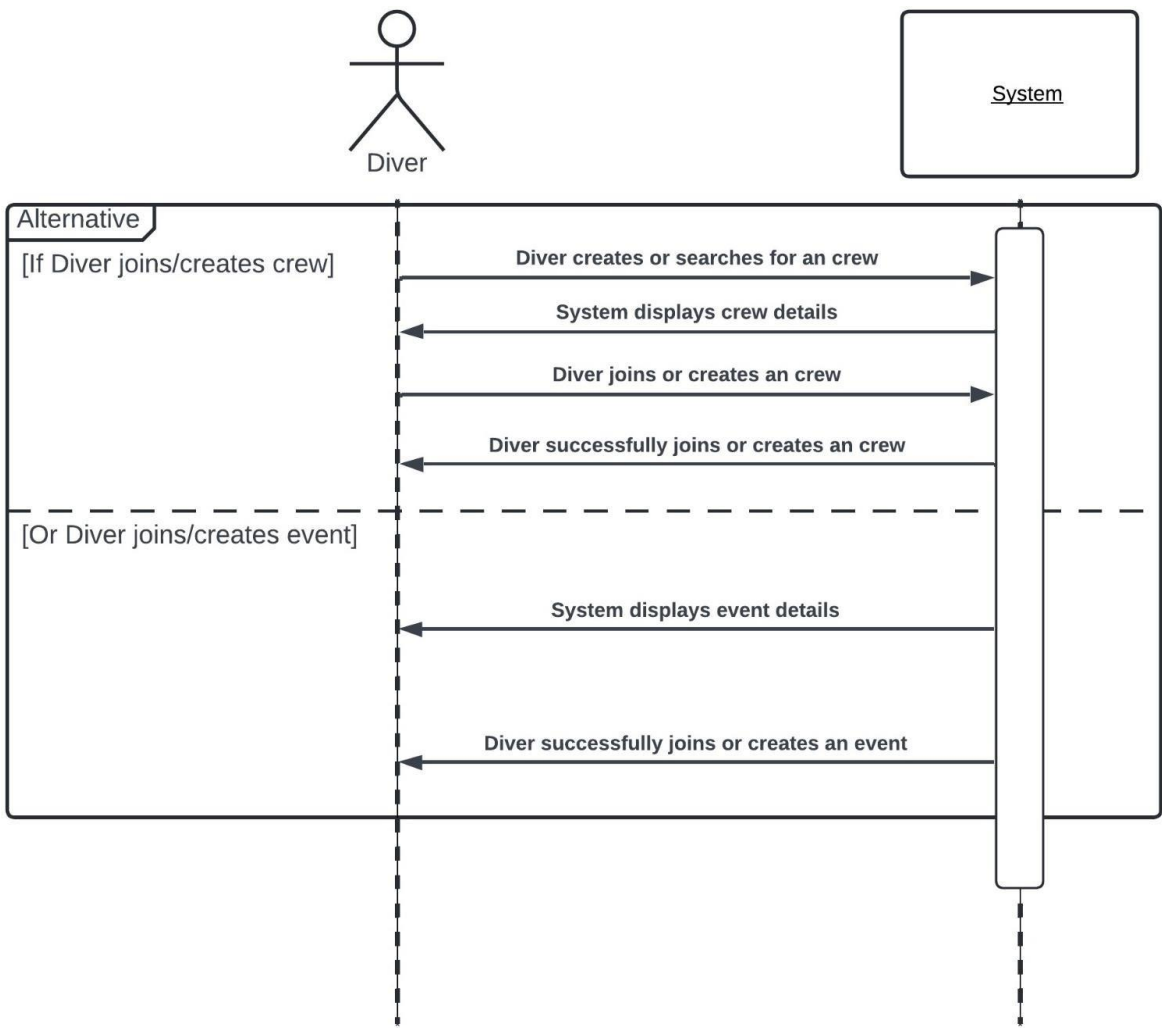
# Sequence Diagram of Use Case 2 - Installing the License



Sequence Diagram of Use Case 10 -Verify Diver Certification

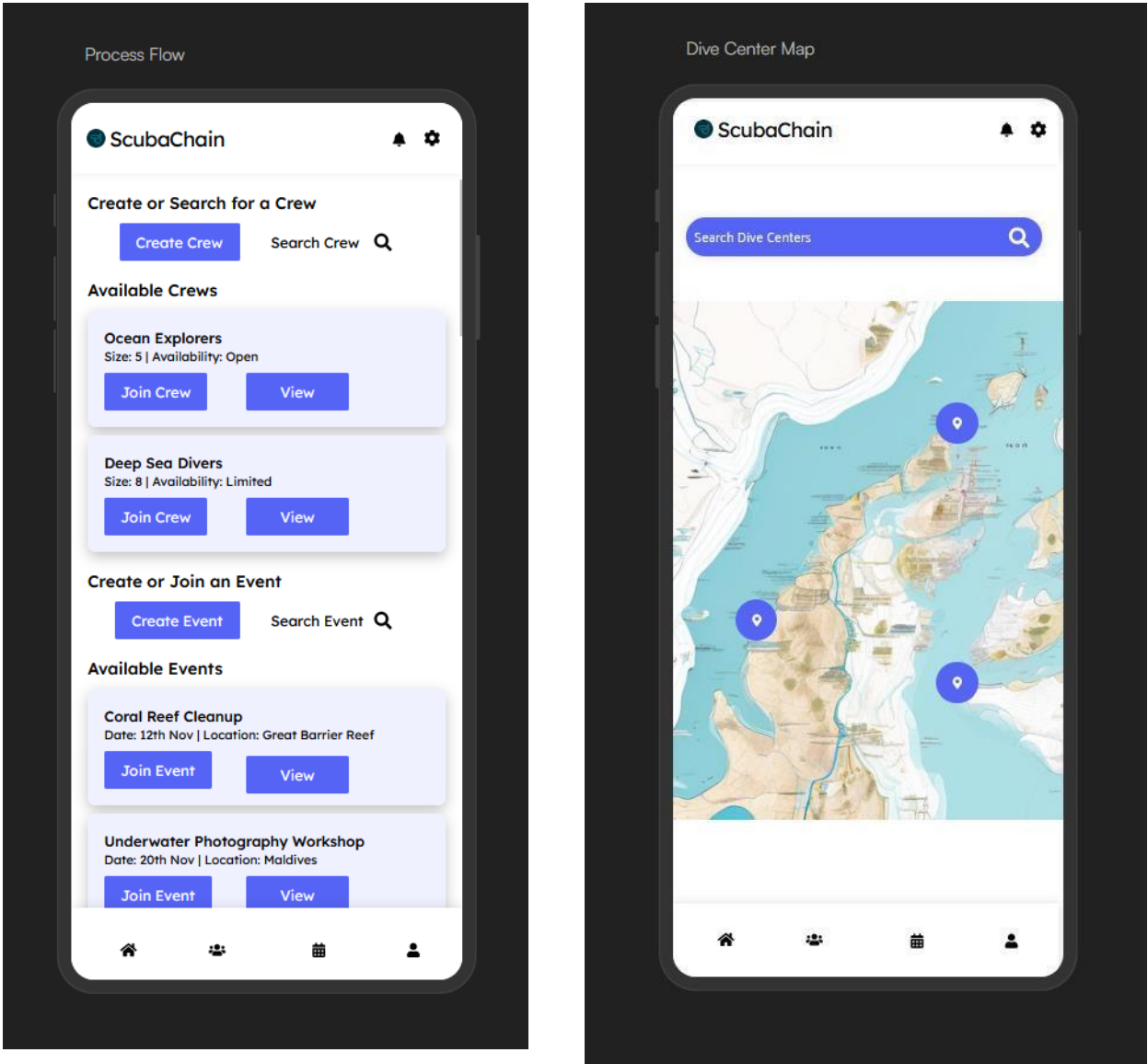


Sequence Diagram of Use Case 9 -Creating/Joining a Crew & Event






### 3. USER INTERFACE (UI) DESIGN



Dive Center Rating Screen

ScubaChain




**Coral Reef Dive Center**  
Bali, Indonesia

Rate your experience:  

Leave a comment...

Submit



**Ocean's Edge Diving**  
Cairns, Australia

Rate your experience:  

Leave a comment...


Submit

Diver Licenses Page

ScubaChain

**Diver Licenses**


**Open Water Diver**



Issuing Agency: PADI  
Date of Issue: 2021-06-15  
Expiration Date: 2024-06-15

Download License


**Advanced Open Water**



Issuing Agency: NAUI  
Date of Issue: 2020-08-22  
Expiration Date: 2023-08-22

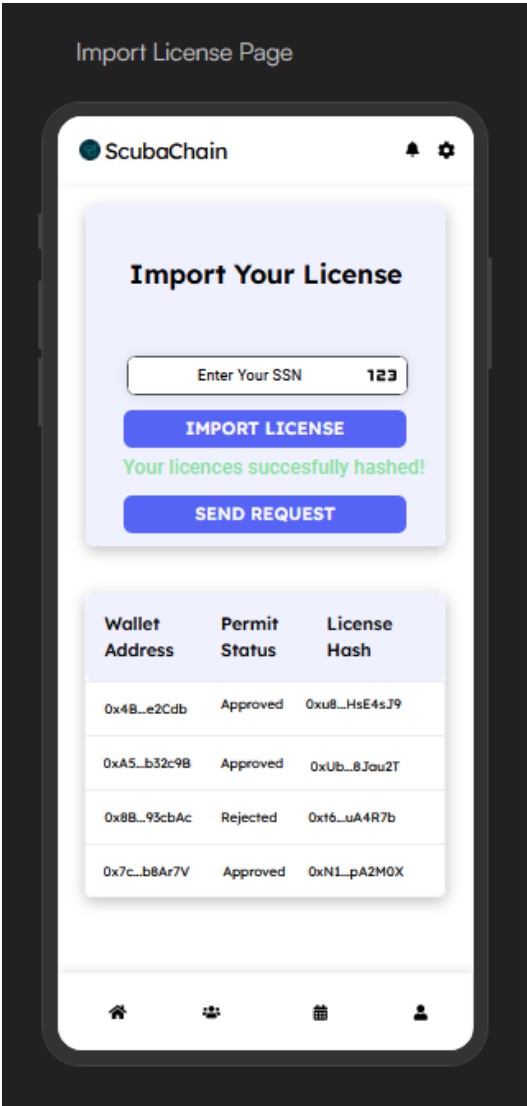
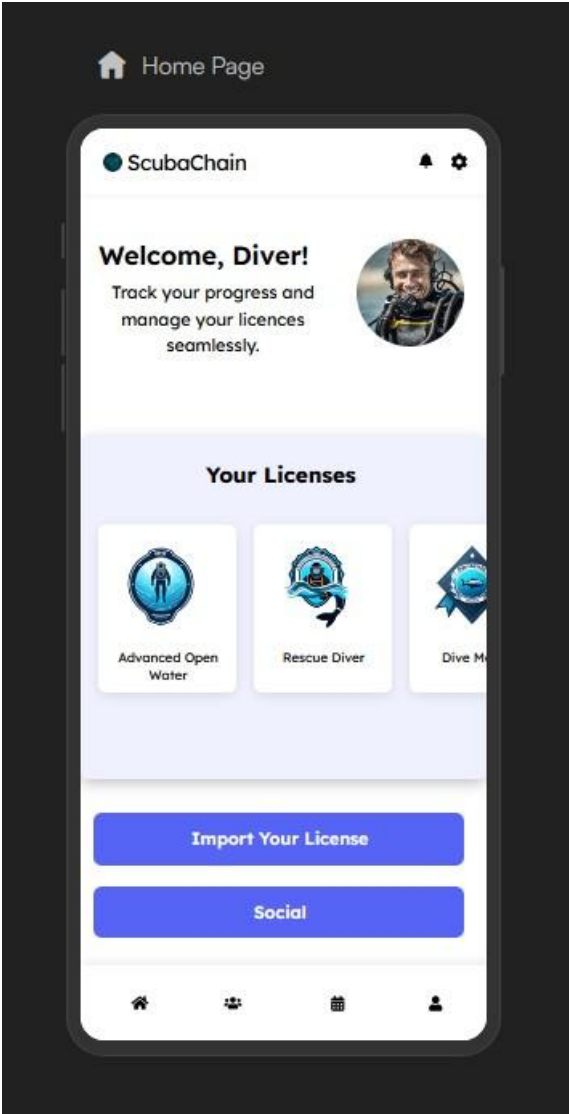
Download License

**Rescue Diver**





Issuing Agency: SSI  
Date of Issue: 2019-11-30  
Expiration Date: 2022-11-30

Download Licenses











## License Verification Page

ScubaChain



### Verify License



Wallet Address	License Hash	Situation
0x4B...e2Cdb	0xA5...b32c9s	 
0xA5...52f9B	0x2B...32cbAv	 
0x8B...93cbAc	0x7C...65cbAc	 
0x7c...b8Ar7V	0x1B...82xfnp	 

< >




## Log Dive Information


ScubaChain




Dive Location

Enter location 

Dive Center

Select Dive Center 

Duration (minutes)



Max Depth (meters)

123


Depth (meters)

123

Visibility

123

Date

mm/dd/yy 

Bottom Time

Enter no

Weight

123

Bar Start

123

Bar End


123

Tempeture


Dive No

Enter no

Time in

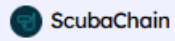


Time Out



Save Dive





## Welcome !

Login with your Metamask to  
access your scuba licenses  
securely.

Connect as Diver

Connect as Dive Center

Connect as Dive Master

Need help? Contact us

By logging in, you agree to our Terms & Conditions

## **Conclusion**

The ScubaChain project demonstrates how blockchain technology can be successfully applied to solve real-world challenges in the scuba diving industry. By transitioning from traditional paper-based systems to a secure, transparent, and tamper-proof digital platform, ScubaChain improves data reliability, reduces administrative burdens, and enhances user experience for divers and dive centers alike.

The project also sets a precedent for future innovations by integrating NFTs, geolocation-based dive site maps, and real-time updates to enrich the diving experience. Through ScubaChain, the diving community can build trust, streamline operations, and foster global connections. As the platform evolves, it is expected to contribute to the standardization of scuba diving certification processes, making the industry more efficient, secure, and sustainable for future generations.

## Reference

[1] T. Sufiyan, "What is node.js? A complete guide for developers," Simplilearn.com, <https://www.simplilearn.com/tutorials/nodejs-tutorial/what-is-nodejs> (accessed Nov. 5, 2024).

[2] A. Sharma, "Express JS tutorial" Simplilearn.com, <https://www.simplilearn.com/tutorials/nodejs-tutorial/what-is-express-js> (accessed Nov. 5, 2024).

[3] M. Sharma, "Difference between web 1.0, web 2.0, and web 3.0," GeeksforGeeks, <https://www.geeksforgeeks.org/web-1-0-web-2-0-and-web-3-0-with-their-difference/> (accessed Nov. 4, 2024).

[4] "What is OpenZeppelin, and What is Its Purpose?," Openzeppelin, <https://www.openzeppelin.com/about> (accessed Nov. 1, 2024).

[5] "What is solidity?," Alchemy, <https://www.alchemy.com/overviews/solidity> (accessed Nov. 3, 2024).

[6] S. Kumar, "Advantages and disadvantages of solidity," Showwcase, <https://www.showwcase.com/article/25408/advantages-and-disadvantages-of-solidity> (accessed Nov. 3, 2024).

[7] "What is the interplanetary file system (ipfs), and how does it work?," Cointelegraph, <https://cointelegraph.com/learn/what-is-the-interplanetary-file-system-ipfs-how-does-it-work> (accessed Nov. 3, 2024).

[8] AltexSoft, "Pros and cons of Flutter App Development," AltexSoft, <https://www.altexsoft.com/blog/pros-and-cons-of-flutter-app-development/> (accessed Nov. 3, 2024).

[9] GeeksforGeeks, "Features of blockchain," GeeksforGeeks, <https://www.geeksforgeeks.org/features-of-blockchain/> (accessed Nov. 3, 2024).

[10] "The metamask extension: What is MetaMask used for?," Gemini, <https://www.gemini.com/cryptopedia/what-is-metamask-how-to-use-metamask-extension#section-what-is-meta-mask> (accessed Nov. 1, 2024).

[11] "Features," MetaMask developer documentation, <https://docs.metamask.io/snaps/features/> (accessed Nov. 1, 2024).

[12] "What is truffle?," Truffle, <https://archive.trufflesuite.com/docs/truffle/> (accessed Nov. 1, 2024).

[13] "Documentation: Ethereum development environment for professionals by Nomic Foundation," Hardhat, <https://hardhat.org/docs> (accessed Nov. 1, 2024).

[14] <https://ieeexplore.ieee.org/document/278253>

[15] <https://blockchain.ieee.org/standards>

[16] <https://miro.com>

[17] Ethereum.org, “Networks,” ethereum.org, <https://ethereum.org/en/developers/docs/networks/> (accessed Dec. 24, 2024).

[18] “Solidity” Solidity, <https://docs.soliditylang.org/> (accessed Dec. 24, 2024).

[19] “Flutter documentation” Docs, <https://docs.flutter.dev/> (accessed Dec. 24, 2024).

[20] “Node.js V23.5.0 documentation,” Index | Node.js v23.5.0 Documentation, <https://nodejs.org/docs/latest/api/> (accessed Dec. 24, 2024).

[21] “Main page,” PostgreSQL wiki, [https://wiki.postgresql.org/wiki/Main\\_Page](https://wiki.postgresql.org/wiki/Main_Page) (accessed Dec. 25, 2024).

[22] A. Shikalgar, (PDF) a review on “ipfs based decentralized social media platform,” [https://www.researchgate.net/publication/371158121\\_A\\_Review\\_on\\_IPFS\\_Based\\_Decentralized\\_Social\\_Media\\_Platform](https://www.researchgate.net/publication/371158121_A_Review_on_IPFS_Based_Decentralized_Social_Media_Platform) (accessed Dec. 25, 2024).

[23] “Integrate your dapp with the metamask wallet,” MetaMask developer documentation, <https://docs.metamask.io/wallet/> (accessed Dec. 25, 2024).

[24] Official results for JS Web Frameworks Benchmark, <https://krausest.github.io/js-framework-benchmark/index.html> (accessed Dec. 25, 2024).