ÇANKAYA UNIVERSITY

COMPUTER ENGINEERING DEPARTMENT

CENG 407

LITERATURE REVIEW

Adopting Blockchain Technology in Scuba Diving

Deniz KAR

İclal Sezin GÜRSES

Arda Celal KAPLAN

Ahmet Berk EROĞLU

Mustafa Arda ERDİNÇ

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.

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).