**ISOM3000H Final Report**

**AccrediChain - Web3.0 Accreditation System**

**Introduction**

As blockchain enthusiasts and students active in both the technological field and the business world, we are constantly exploring innovative technologies that can solve real-world problems. One area that has caught our attention is the traditional centralized accreditation system, which has limitations such as lack of transparency, limited accessibility, and security concerns. These challenges have led us to research and explore the potential of decentralized accreditation systems, which can offer a more efficient, secure, and transparent approach to accreditation. Our passion for blockchain technologies and our desire to create meaningful solutions for real-world problems has motivated us to undertake a project in this area.

**Our Group**

The workload of our group was equally distributed, with each member contributing their expertise in different areas.

HEUNG Kai Him (Anson) is responsible for the frontend development and handling API calls. With his skills and experience, he ensures that our platform's frontend is user-friendly and accessible, allowing for seamless interaction with the backend.

LEE Ho Wan Owen is in charge of the smart contract development and the architectural design of our platform. He has developed an intermediate level of understanding in Solidity programming within the short span of weeks and has contributed significantly to the design of our data structures.

CHUI On Lam (Rachel) is responsible for the business presentation, report writing, and end-to-end code testing. She plays a crucial role in identifying new use cases and develops strategies for the expansion of our platform. She has also conducted extensive testing to ensure that our platform is secure and reliable.

Each member worked diligently to ensure the success of the project and collaborated effectively to bring the decentralized accreditation system to fruition.

**Situational Analysis**

**Market Analysis**

The current market size for accreditation is substantial and expected to continue expanding in the years to come. The global certification market was valued at USD 167.78 billion in 2020 and is projected to grow at a CAGR of 7.8%, reaching USD 308.98 billion by 2028. The market's growth is fueled by the increasing demand for skilled professionals and compliance with industry standards and regulations across different sectors. A 2020 survey by the HR Certification Institute showed that 80% of US organizations rely on centralized certification systems to evaluate the skills and qualifications of their employees or job candidates, and 84% of HR professionals view certification as an important criterion for hiring. Certification programs are offered by educational institutions, professional associations, and industry-specific organizations, among others. However, the traditional centralized certification systems face several challenges, such as limited accessibility, lack of transparency, and security concerns, creating a need for more innovative and decentralized solutions.

Hong Kong is the perfect place to launch a decentralized accreditation system given its reputation as a hub for innovation and technology. The demand for such a system is also evident as Hong Kong's Quality Assurance industry has been identified as one of the six potential growth industries alongside the four pillar industries. With the support of the Hong Kong government and its commitment to nurturing the innovation and technology ecosystem, the potential for our decentralized accreditation system in the local market is significant.

**Challenges with traditional certification system**

The traditional certification system has some limitations that make it less effective in today's digital age. Some of the problems with traditional certifications are:

1. **Lack of transparency:** Conventional certifications are often issued by centralized authorities, which can make the process less transparent and open to abuse. In 2018, the New York Times reported on the fraudulent practices of a prominent certification body in the US, which raised concerns about the lack of transparency and accountability in the certification industry. The opacity in the field creates opportunities for fraudulent activities, such as the creation of fake certificates or the manipulation of records. This can have serious consequences, particularly in industries where safety and quality standards are critical, such as healthcare or aviation.
2. **Limited accessibility:** Acquiring traditional certificates can be costly, which can impede individuals and organizations in their pursuit of authenticating their qualifications. The average cost of obtaining a certification in the US is around $1,000 with reference to a report by the Lumina Foundation, which can be a significant barrier for individuals from low-income backgrounds. Furthermore, conventional certification programs can be time-consuming and require physical attendance, which may not be feasible for individuals with work or family commitments. This can limit accessibility and exclude qualified individuals from obtaining certifications.
3. **Limited portability:** The transferability of traditional certifications is restrictive, as they often only apply to specific industries or geographic locations, which limits the utility of these certifications across different settings and constrains individuals' ability to leverage their qualifications in diverse contexts. This can create challenges for individuals seeking to transition between industries or regions, where their existing certifications may not be recognized or valued.
4. **Limited security:** Security is a major concern of traditional certification systems, as they can be vulnerable to counterfeiting and fraudulent practices, which can erode their credibility and reliability. A study by Credential Engine revealed that credential fraud is a mounting issue in the US, with roughly 40% of resumes including fabricated or embellished credentials. Additionally, the BBC reported on the prevalence of fake degrees in Pakistan, where unaccredited institutions offer counterfeit degrees with ease. As a result, the authenticity and integrity of traditional certification systems are being called into question, necessitating more secure and reliable alternatives such as decentralized certification systems.

**Solution**

Our proposed solution is a decentralized accreditation system built on blockchain technology, which provides a transparent, secure, and accessible way for individuals and organizations to obtain and verify certifications. This system would leverage smart contracts and a shared database to ensure the accuracy and validity of certifications, while also democratizing access to certification by reducing barriers to entry.

**Need for Decentralization**

Decentralization is needed in certification because traditional centralized certification systems are limited in their ability to address key issues such as fraud, inaccessibility, and lack of transparency. By adopting a decentralized approach, these issues can be effectively addressed through the following:

1. **Shared database:** A decentralized system allows for the creation of a shared tamper-proof database that all parties have access to. This ensures that the accuracy and validity of certifications are maintained, and any attempts at fraudulent activity are immediately detected and addressed.
2. **Multiple writers:** In a decentralized system, multiple writers can contribute to the shared database, making the accreditation process more efficient and ensuring that all stakeholders have a say in the process.
3. **Absence of trust:** A decentralized system eliminates the need for trust in third-party intermediaries, such as certification authorities or verification services, by allowing all parties to verify each other's credentials directly.
4. **Disintermediation:** Our decentralized accreditation system eliminates intermediaries, such as educational institutions, professional associations, or third-party verification services to issue, apply and validate certifications, reducing administrative overhead and making the accreditation process more efficient and cost-effective. This also enhances transparency and validity, without the need for costly third-party verification. It enables a direct connection between the issuer and holder, increasing accuracy and control over the verification process.
5. **Transaction interaction:** A decentralized system allows for direct interaction between parties in the certification process, making it easier to track and verify credentials across different industries and regions. This enhances the portability of certifications and increases their overall value.

**Workflow**

The workflow of our decentralized accreditation system involves three key players: the certificate issuer, certificate applicant, and certificate verifier.

The certificate issuer is responsible for launching the accreditation process and issuing certificates to successful applicants. This is done through the use of smart contracts, which are self-executing programs that automate the verification and issuance of certifications. Once a certification is issued, it is stored on a shared database accessible by all parties.

Certificate applicants can apply for accreditation through the system, submitting their qualifications and credentials for verification. Once their application is approved, they receive their certificate, which is also stored on the shared database.

Certificate verifiers can access the shared database to verify the ownership and issuance of certificates. This allows for remote and flexible verification, as verifiers can access the database from anywhere at any time.

The use of blockchain technology ensures the integrity and immutability of the certification records, preventing fraud and counterfeiting. Additionally, the elimination of intermediaries and administrative overhead results in a more cost-effective and efficient accreditation process.

**Business Model**

The business model for our decentralized accreditation system involves generating revenue through three primary sources. Firstly, the certificate issuer pays a fee to us for the issuance of accreditations, which allows them to leverage the benefits of the system. Secondly, verifiers pay a verification fee to access and verify certification records stored on the system. For example, a company may want to validate the authenticity of an employee's employment certificate. Lastly, we can earn revenue by displaying ads on the frontend of our platform. Companies can pay us a fee to advertise their products or services related to the certifications offered on our platform. For instance, ads promoting IELTS courses can be displayed on a page about IELTS certifications. These revenue streams will help us sustain the platform and continuously improve its features and functionalities.

**Advantages**

Web3.0 accreditation system addresses these limitations by using blockchain technology, which provides a decentralized and transparent platform for verifying credentials. The advantages of our Decentralized Accreditation System are:

1. **Improved transparency:** Our system ensures the accuracy and validity of certifications by providing a shared tamper-proof database accessible to all parties involved in the accreditation process. This promotes transparency and trust in the system, eliminating the possibility of fraudulent activities and false claims.
2. **Increased accessibility:** Our Decentralized Accreditation System provides a more accessible approach to obtaining and verifying credentials. With remote and flexible verification options, individuals can easily share their certifications from anywhere at any time, reducing the need for physical attendance and travel expenses. It also eliminates intermediaries and administrative overhead, resulting in a more cost-effective and efficient accreditation process. This reduces the financial burden on individuals and organizations seeking to verify their credentials, making the accreditation process more accessible and affordable for all.
3. **Greater portability:** Certifications obtained through our system are not limited to specific industries or regions, allowing individuals to use their credentials in diverse settings. This increases the value and recognition of certifications, providing individuals with more opportunities for career advancement and professional development.
4. **Enhanced security:** The use of blockchain technology in our system ensures the integrity and immutability of certification records, making them resistant to tampering and hacking attempts. This provides a high level of security for sensitive personal information and ensures that certification records cannot be altered or deleted once added to the blockchain.

Our Decentralized Accreditation System provides a more reliable, accessible, and secure way to verify credentials in the digital age, which is essential for building trust and promoting transparency in various industries and contexts.

**Implementation**

Our decentralized accreditation system is a full-stack platform that seamlessly integrates both the frontend and the backend to create a unified user experience. Our implementation can be found on our [Github repository](https://github.com/olchui428/isom3000h-project.git) which has been deployed on <https://isom3000h-project-6ijv-274ayojj3-isom3000.vercel.app/>.

**Frontend**

The frontend is built using Next.js and is styled using the Material UI (MUI) framework. The frontend is designed to be user-friendly, allowing users to easily navigate and interact with the system. The frontend provides various features such as user registration for both issuers and applicants, certificate issuance, certificate verification, and user profile management.

The frontend interacts with the blockchain via the MetaMask browser extension. To minimize developer overhead and compartmentalize all blockchain interactions, all blockchain information and interaction functions are implemented on an external hook dubbed “useMetaMask”, while only exposing high-level descriptive functions names to the frontend developer so that future frontend developers can still implement features regardless of their knowledge and background in blockchain programming.

On our platform's homepage, users can easily access accreditation and certificate details by entering their ID, or searching for registered certificate issuers and applicants using their wallet address. These actions can be performed without the need to connect a Metamask wallet.

For certificate issuers and applicants who wish to register and perform additional actions on the platform, our frontend allows for Metamask wallet connection. Upon successful registration, issuers can launch accreditations for future certificate issuance, details are described in the "Data Structure" section. Once an accreditation category is created, certificates can be issued to registered applicants via their Metamask wallet address. As a certificate applicant, all issued certificates can be conveniently viewed under the "My Certificates" tab.

As a way to enhance user experience, we have added a new feature that generates certificate images. In the certificate verification page, a “Download Certificate” button is introduced to let users view a dynamically generated image of a certificate containing all relevant information and details. The certificate image generation process is initiated by passing the certificate ID to the designated API route on Next.js. A JsonRpcProvider object connected to the blockchain is then created to retrieve relevant certificate data, which is then printed to a blank certificate image template using an npm package @napi-rs/canvas that provides a set of image processing APIs identical to that of HTML5 Canvas. A Buffer object of the generated image is then returned via HTTP response, allowing the user to view the image in PNG or JPG format in the frontend.

**Backend**

The backend of the platform consists of 10 smart contracts written in Solidity, which are responsible for managing the accreditation process. The smart contracts adopt a modular design, meaning that each contract performs only one specific function to prevent code cluttering and to improve the ease of debugging and refactoring. The smart contracts include four storage contracts, two NFT (Non-Fungible Token) contracts, and four endpoint contracts. All contracts apart from the endpoint contracts have implemented access control, i.e. the functions on these contracts can only be called from explicitly allowed contract addresses. These contracts are deployed using Hardhat, with the production environment being the ETD Debug Chain. We also conduct testing on the Mumbai Testnet and locally using Ganache to ensure the reliability and accuracy of the platform.

The storage contracts each act as a database table and are responsible for storing accreditation data, the details of which shall be elaborated in the next section “Data Structure”. The NFT contracts are used to represent the certificates as unique digital assets that can be issued to the applicant and verified on the blockchain. The endpoint contracts provide the necessary functions for certificate issuers, certificate holders, and verifiers to interact with the system.

We adopt the OpenZeppelin implementation of the ERC721 contract for making NFT smart contracts in our decentralized accreditation system because ERC721 is a widely accepted standard for creating unique, digital assets on the Ethereum blockchain. It provides a high level of customization and flexibility, allowing us to create unique and specific attributes for each accreditation or certification. It enables us to create unique digital identities for each certification, which is critical in preventing fraud and ensuring the integrity of the system. Furthermore, ERC721 provides a standard for how NFTs can be minted, issued and potentially burned, which is important for users to own and manage these unique digital assets on their digital wallets. Overall, using ERC721 provides a secure and standardized way of creating and managing digital assets, which is crucial for the success of our decentralized accreditation system.

The platform's backend is designed to operate on a decentralized blockchain network, allowing for greater transparency, security, and efficiency. The use of smart contracts ensures that the accreditation process is tamper-proof and cannot be manipulated, providing greater confidence in the validity and accuracy of the certifications.

**Data Structure**

In our decentralized accreditation system, 4 entities are stored and managed, namely Issuer, Applicant, Accreditation and Certificate. The details and differences of Issuer and Applicant have been described in detail in previous sections.

Accreditation is a collection or category of certificates that is created by the issuer, for instance examinations such as HKDSE and quality standards such as those defined under ISO. It contains attributes such as the issuer, title, creation time, duration, description, nature, and other relevant information. An Accreditation can be created by an issuer and is a prerequisite for creating a Certificate.

| struct Accreditation {  /// @param id NFT token ID, globally unique  uint256 id;  /// @param issuer Address of Accreditation Issuer  address payable issuer;  /// @param title Title/name of Accreditation  string title;  /// @param createdAt The UTC time of creation of Accreditation / 1000  uint256 createdAt;  /// @param duration Duration of Accreditation before expiry, stored in the number of seconds. 0 if no expiry date  uint256 duration;  /// @param nature Nature of Accreditation, e.g. Participation, Award, Achievement, Graduation, Exam, etc.  string nature;  /// @param description Textual description of the Accreditation  string description;  /// @param isRevoked (Optional) Boolean to show if this Accreditation was revoked, default value false  bool isRevoked;  /// @param revokeReason (Optional) Reason why this Accreditation was revoked, if it is, otherwise stay blank  string revokeReason;  /// @param revokeTime (Optional) Timestamp when this Accreditation was revoked, if it is. Default value = 0  uint256 revokeTime;  } |
| --- |

*Data structure of Accreditation*

On the other hand, a Certificate is a child of an Accreditation that is created by the issuer and owned by the certificate applicant. It contains attributes such as the issuer, applicant, accreditation ID, level, createdAt, and other relevant information. A Certificate can only be created by an issuer who has already created an Accreditation. Once a Certificate is created, it can be transferred to the certificate applicant.

| struct Certificate {  /// @param id NFT token ID, globally unique  uint256 id;  /// @param issuer Address of Accreditation Issuer  address payable issuer;  /// @param applicant Address of Certificant recipient  address payable applicant;  /// @param createdAt The UTC time of creation of Certificate / 1000  uint256 createdAt;  /// @param accreditationId NFT token ID of the corresponding Accreditation, acts as foreign key  uint256 accreditationId;  /// @param level The level of achievement of this certificate, e.g. "Pass", "Distinction", "Listening - 9.0\nReading - 9.0\nWriting - 8.0\nSpeaking - 8.0", use '\n' to separate if multiple lines  string level;  /// @param eventId (Optional) ID of the organization internal database  string eventId;  /// @param remarks (Optional) Remarks or words of encouragement, if the Issuer wishes to add any on the certificate  string remarks;  /// @param isRevoked (Optional) Boolean to show if this Certificate was revoked, default value false  bool isRevoked;  /// @param revokeReason (Optional) Reason why this Certificate was revoked, if it is, otherwise stay blank  string revokeReason;  /// @param revokeTime (Optional) Timestamp when this Certificate was revoked, if it is. Default value = 0  uint256 revokeTime;  } |
| --- |

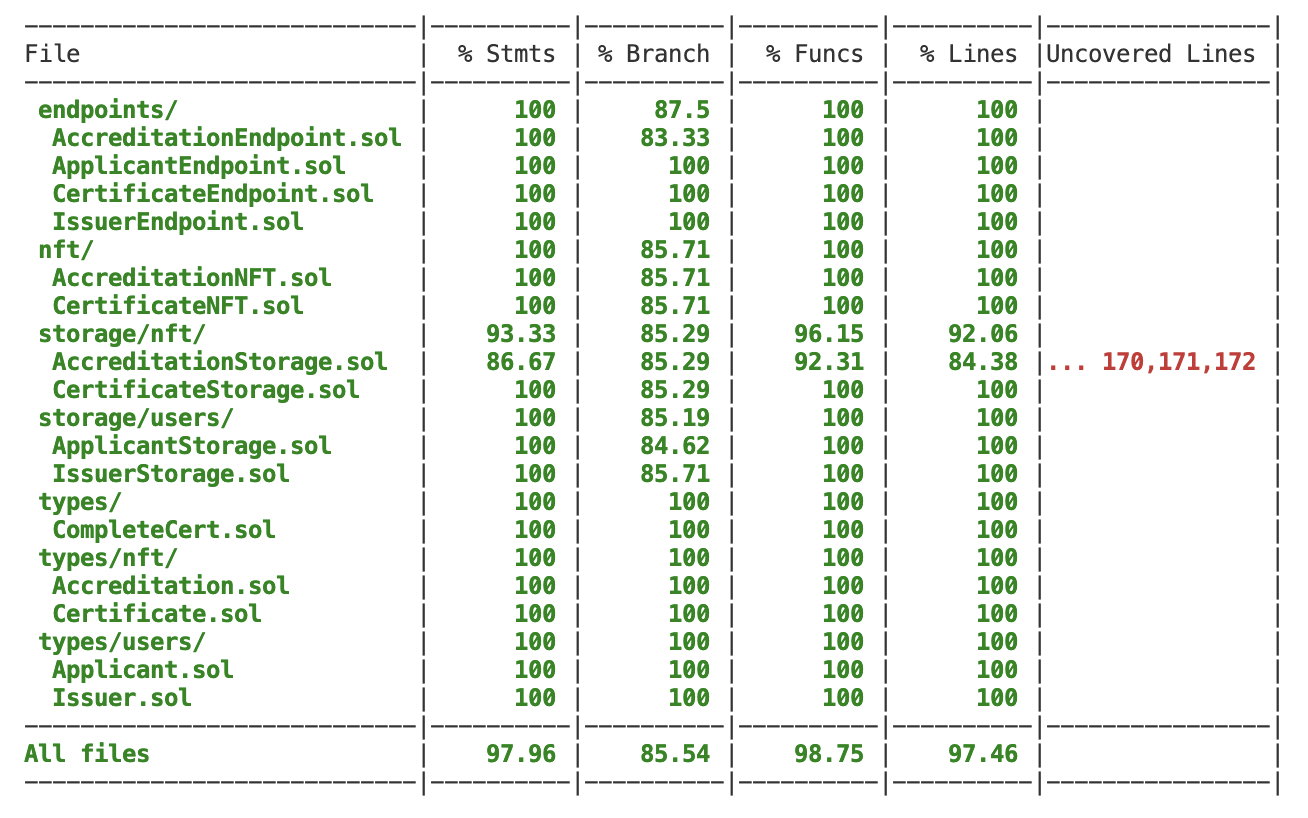
*Data structure of Certificate*

When an issuer creates a certificate, it is minted as a unique NFT on the blockchain which contains all the relevant information about the certificate. The NFT can then be issued to the certificate applicant, making the applicant the owner of the certificate.

The data structure of our certificates ensures that every Certificate is associated with a valid Accreditation, is issued by and to valid users, and provides a clear and traceable record of the certification process.

**Testing**

Extensive testing has been performed on all branches and statements of each smart contract. The tests are done under several environments including Mumbai Testnet and the local chain from Ganache.



*Testing coverage with hardhat*

Below shows the complete workflow of the system, which consists of registration of issuers and applicants, launching accreditations and issuance of certificates, as well as validation of certificates. The smart contracts and its usage have been proven to be error-free and the performance shown to be at an acceptable speed.

| > check:local  > hardhat run scripts/check.ts --network local  Setting up Contracts  Successfully set up Contracts  Setting up accounts  Successfully set up accounts  Start checking:  Checking IssuerEndpoint::registerIssuer()  Successfully registered Issuer  Registered Issuer: ABC Company,0x41c1AA19E51C5B6341aff7d0e42CF1a820A8Cb39,It is a good company,https://picsum.photos/200/300,1683782988  Checking ApplicantEndpoint::registerApplicant()  Successfully registered Applicant 1  Successfully registered Applicant 2  Registered Applicant 1: Owen Lee,0x241f7dD6e93b7aD0Ee13E448eAfFaaF66AEFae2E,1683782989  Registered Applicant 2: Amy Chan,0xbc96881548a17BeAe9e17cBA0b942C9811c7A3bC,1683782989  Checking AccreditationEndpoint::launchAccreditation()  Successfully launched Accreditation  Launched Accreditation: 0,0x41c1AA19E51C5B6341aff7d0e42CF1a820A8Cb39,HKDSE,888,1,Exam,It is a tough exam.,false,,0  Checking CertificateEndpoint::issueCertificate()  Successfully issued Certificate 1 to Applicant 1  Successfully issued Certificate 2 to Applicant 2  CompleteCert 1: ABC Company, 0x41c1AA19E51C5B6341aff7d0e42CF1a820A8Cb39, It is a good company, <https://picsum.photos/200/300>, 1683782988, Owen Lee, 0x241f7dD6e93b7aD0Ee13E448eAfFaaF66AEFae2E, 1683782989, 0, 0x41c1AA19E51C5B6341aff7d0e42CF1a820A8Cb39, HKDSE, 888, 1, Exam, It is a tough exam., false, , 0, 0, 0x41c1AA19E51C5B6341aff7d0e42CF1a820A8Cb39, 0x241f7dD6e93b7aD0Ee13E448eAfFaaF66AEFae2E, 1683782988296, 0, 5\*\*, 777, Good, false, , 0  CompleteCert 2: ABC Company, 0x41c1AA19E51C5B6341aff7d0e42CF1a820A8Cb39, It is a good company, <https://picsum.photos/200/300>, 1683782988, Amy Chan, 0xbc96881548a17BeAe9e17cBA0b942C9811c7A3bC, 1683782989, 0, 0x41c1AA19E51C5B6341aff7d0e42CF1a820A8Cb39, HKDSE, 888, 1, Exam, It is a tough exam., false, , 0, 1, 0x41c1AA19E51C5B6341aff7d0e42CF1a820A8Cb39, 0xbc96881548a17BeAe9e17cBA0b942C9811c7A3bC, 1683782988296, 0, 2, 778, Poor, false, , 0  Completed in 7.13 seconds. |
| --- |

*Testing entire workflow on Ganache*

**Reflection & Concluding Remarks**

As we reflect on the development and implementation of our decentralized accreditation system, we are proud of the progress we have made in creating a more accessible, transparent, secure, and portable system for validating certifications. However, we recognize that there is still room for improvement and expansion. We believe that by further integrating our system with other industries and institutions, we can enhance its functionality and increase its impact.

With the increasing demand for skilled professionals, our decentralized accreditation system has the potential to transform the hiring process by making it more efficient and accurate. Through our platform, recruiting companies can easily verify the authenticity of candidates' certifications and credentials, and identify the best candidates for specific job positions. This can save time and resources for companies and improve the chances of finding the most qualified candidates.

Moreover, our system can provide universities with valuable insights into the performance of their students. By linking certificates to specific courses, universities can obtain statistics on the performance and outcomes of their students in various courses. This can help universities to make data-driven decisions about course offerings, curriculum development, and academic programs.

In addition to its potential in the job market and academia, our decentralized accreditation system can also be utilized for mortgage and other financial applications. A decentralized accreditation system can be used to verify and authenticate certifications related to a person's financial history, which can be useful in the mortgage application process. For example, a mortgage lender could use the system to verify a borrower's income and employment history, which is often required during the underwriting process. This verification process could be simplified and streamlined by relying on the decentralized system, which eliminates the need for multiple parties and intermediaries to verify the information. Additionally, the system could also be used to verify a borrower's credit history and other financial information, making the mortgage application process faster and more secure.

Overall, we are excited about the potential of our decentralized accreditation system to transform various industries and applications. We will continue to explore and develop new use cases for our system to maximize its benefits for all parties involved.