VIVEKANAND EDUCATION SOCIETY'S
INSTITUTE OF TECHNOLOGY

Department of Computer Engineering

Project Report on

DeCAT -Decentralized Certificate Authority

In partial fulfillment of the Fourth Year (Semester–VII), Bachelor of Engineering

(B.E.) Degree in Computer Engineering at the University of Mumbai Academic Year 2023-2024

Dr.(Mrs.) Nupur Giri

Submitted by

Varad Deshmukh (D17B / 22), Dhananjay Pai (D17B / 50),
Hrishikesh Patil (D17B / 54), Yash Sahane (D17B/60)

(2023-24)

VIVEKANAND EDUCATION SOCIETY'S
INSTITUTE OF TECHNOLOGY
Department of Computer Engineering

CERTIFICATE of Approval

This is to certify that _____of Fourth Year Computer Engineering studying under the University of Mumbai has satisfactorily presented the project on "***DeCAT -Decentralized Certificate Authority***" as a part of the coursework of PROJECT-I for Semester-VII under the guidance of ***Dr.(Mrs.) Nupur Giri*** in the year 2023-2024.

_____

Date

_____ _____

Internal Examiner External Examiner

_____ _____ _____

Project Mentor Head of the Department Principal

Dr. Mrs. Nupur Giri Dr. J. M. Nair

ACKNOWLEDGEMENT

We are thankful to our college Vivekanand Education Society's Institute of Technology for considering our project and extending help at all stages needed during our work of collecting information regarding the project.

It gives us immense pleasure to express our deep and sincere gratitude to **Dr.(Mrs.) Nupur Giri .** for her kind help and valuable advice during the development of project synopsis and for her guidance and suggestions.

We are deeply indebted to Head of the Computer Department **Dr.(Mrs.) Nupur Giri** and our Principal **Dr. (Mrs.) J.M. Nair,** for giving us this valuable opportunity to do this project.

We express our hearty thanks to them for their assistance without which it would have been difficult in finishing this project synopsis and project review successfully.

We convey our deep sense of gratitude to all teaching and non-teaching staff for their constant encouragement, support and selfless help throughout the project work. It is a great pleasure to acknowledge the help and suggestion, which we received from the Department of Computer Engineering.

We wish to express our profound thanks to all those who helped us in gathering information about the project. Our families too have provided moral support and encouragement several times.

Computer Engineering Department

COURSE OUTCOMES FOR B.E PROJECT

Learners will be to:-

Course Outcome	Description of the Course Outcome
CO 1	Do literature survey/industrial visit and identify the problem of the selected project topic.
CO2	Apply basic engineering fundamental in the domain of practical applications for problem identification, formulation and solution
CO 3	Attempt & Design a problem solution in a right approach to complex problems
CO 4	Cultivate the habit of working in a team
CO 5	Correlate the theoretical and experimental/simulations results and draw the proper inferences
CO 6	Demonstrate the knowledge, skills and attitudes of a professional engineer & Prepare report as per the standard guidelines.

INDEX

Chapter No.	Title	Page No.
1	**Introduction**	7
1.1	1.1. Introduction to the project	7
1.2	1.2. Motivation for the project	7
1.3	1.3. Problem Definition	8
1.4	1.4. Relevance of the Project	9
1.5	1.5. Methodology Employed	10
2.	Literature Survey 2.1. Research Papers a. Abstract of the research paper b. Inference drawn from the paper 2.2. Books / Articles referred / news paper referred 2.3. Interaction with domain experts.	11
3.	Requirement Of Proposed System 3.1 Functional Requirements 3.2. Non-Functional Requirements 3.3. Constraints 3.4. Hardware & Software Requirements 3.5. Techniques utilized till date for the proposed system 3.6. Tools utilized till date for the proposed system 3.7. Project Proposal	18
4.	Proposed Design 4.1 Block diagram representation of the proposed system Explanation for the block diagram 4.2. Modular diagram representation of the proposed system Explanation for the modular block diagram 4.3 Design of the proposed system with proper explanation of detailed design	27

5.	Results and Discussions	36
6.	Plan Of Action For the Next Semester 6.1.Work done till date 6.2.Plan of action for project II	38
7.	Conclusion	38
8.	Appendix 8.1.List Of Figures	41

Chapter 1 : Introduction

1.1 Introduction

In an era marked by digital transformation, the traditional methods of issuing and verifying certificates, achievements, and credentials face escalating challenges. Concerns surrounding authenticity, tampering, and redundancy undermine the credibility of individuals' accomplishments. To address these issues, the project “DeCAT-Decentralized Certificate Authority” proposes a pioneering solution that leverages the power of blockchain technology and non-fungible tokens (NFTs).This project aims to revolutionize the way certificates and achievements are managed, ensuring the security, integrity, and traceability of each credential. By building a decentralized application (Dapp) on a private blockchain, this initiative introduces a seamless and robust system where issuers can create SoulBound NFTs—tokens that carry unalterable attributes—representing certificates and achievements. Unlike traditional digital certificates, SoulBound NFTs are equipped with unique identities and tamper-resistant properties, making them a trustworthy representation of an individual's accomplishments.The integration of blockchain technology ensures that each NFT's origin, history, and attributes are recorded transparently and immutably. This transparency fosters trust among employers, educational institutions, and other entities requiring verified credentials. Additionally, by developing this solution on a private blockchain, the project retains control over access and enhances privacy while maintaining the benefits of blockchain-based verification.

1.2 Motivation

The increasing trend of global mobility in both the education and professional sectors has led to a growing number of individuals pursuing studies and careers abroad. This has consequently placed a heightened importance on the verification of academic and professional credentials by both employers and educational institutions. Simultaneously, students are required to share personal information, including financial details and academic records, with higher education institutions. It is imperative that this information is securely stored, remains unaltered, and can be easily verified. Unfortunately, there is a prevalent issue of individuals falsifying certificates in order to gain employment or admission, posing a significant challenge for organizations in verifying the legitimacy of these documents. In response to these challenges, secure certificate verification systems have been introduced to effectively manage and authenticate certificates.

1.3 Problem Definition

The current landscape of issuing and verifying certificates, achievements, and other credentials is plagued by issues such as duplication, editing, and lack of trustworthiness which undermines the value and credibility of prestigious accomplishments. This has led to increased redundancy and lowered the value of prestigious achievements. Additionally, individuals can easily fake their portfolios, leading to a lack of confidence in their claims. These issues not only create redundancy but also erode confidence in individuals' claims and portfolios, leading to an urgent need for a more secure and reliable system.

To address these challenges, we aim to build a Decentralized Application on top of L2 blockchain, leveraging Soul Bound NFTs (a modified version of ERC721) to issue certificates and achievements securely. The Soul Bound NFTs act as identity tokens that cannot be transferred or burnt once minted to a user's address, ensuring their authenticity and uniqueness.

1.4 Relevance of the Project

A. Ensuring Authenticity

The project directly addresses the issue of authenticity in digital achievements. By employing blockchain technology and the unique characteristics of SBTs, the system ensures that once an achievement is recorded on the blockchain, it is immutable and secure. This guarantees the authenticity of an individual's portfolio.

B. Fostering Trust

In a world where trust is paramount, especially in professional and academic spheres, the project aims to rebuild confidence in digital credentials. The transparent and decentralized nature of blockchain ensures that the information presented by individuals is reliable, contributing to a trustworthy ecosystem.

C. Scalability and Efficiency

The incorporation of multi-batch transactions and rollup mechanisms reflects the project's commitment to scalability. As the number of users and transactions increases, the system remains efficient, providing a seamless experience for both issuers and recipients.

D. Future-Proofing Credentials

As technology evolves, the project's reliance on blockchain ensures that digital credentials remain relevant and secure. The decentralized nature of the system mitigates the risk of a single point of failure, contributing to the long-term viability of the platform.

1.5 Methodology used

The methodology of the is divided into two types of users:

1. Soul Bound Token Issuer-

   A. The issuer takes care of the verification and authentication of the achievement of the respective receiver using authentication protocol (World Coin) which will be hard-coded in the initial stages

   B. The issuer imports the dataset which contains all the necessary information about the receiver entities for further verification.

   C. All the metadata regarding the user assets(certificates,credentials) will be stored using an interplanetary file system(IPFS).

   D. After the verification and authentication processes, the issuer finally sends the respective soul bound tokens(SBT) to all the wallet addresses from the imported dataset which are valid and verified.

2. SBT Receiver-

   A. The issuer just has to provide the necessary information such as wallet address, credentials and other information to the organization.

   B. Users can see the received SBT in any open NFT marketplace such as OpenSea and showcase it . That NFT is now the identity and proof that the claimed credentials and assets are officially and legally of that receiver.

Chapter 2: Literature Survey

2.1 Research Papers referred

1.Batch Minting-enabled Digital Certificates Based on Soulbound Token for Achievement Verification

[6]Ansori, Muhammad Rasyid Redha, Revin Naufal Alief, Ikechi Saviour Igboanusi, Jae Min Lee, and Dong-Seong Kim. "Batch Minting-enabled Digital Certificates Based on Soulbound Token for Achievement Verification." 한국통신학회 학술대회논문집 (2023): 1350-1351.

Abstract:

This paper introduces a blockchain-based solution that utilizes Soulbound Tokens (SBTs) to enhance the authentication of digital certificates while streamlining the verification process. Conventional methods for certificate verification, which rely on paper-based documentation, often suffer from inefficiencies, errors, and susceptibility to fraud. In contrast, the proposed approach harnesses decentralized and immutable blockchain technology to ensure the secure and transparent authentication of certificates. Under this system, individuals register their addresses with a program manager, and digital certificates are generated and organized in batches through a smart contract. Verifiers can then employ the smart contract's verification function to confirm the authenticity and legitimacy of certificates. Experimental results conducted on the Ethereum blockchain network highlight the cost-efficiency of batch certificate minting, significantly reducing transaction fees as the number of certificates increases.

Inferences:

- Introduction of a novel method for batch minting digital certificates using Soulbound Tokens (SBTs) for achievement authentication.
- Conventional paper-based certificate verification methods are inefficient and susceptible to errors and fraud.
- Blockchain technology and SBTs offer a secure and transparent solution for certificate authentication.

- Elimination of risks related to certificate loss or damage and cost-effective batch minting of digital certificates.
- Demonstrated efficiency through reduced certificate creation costs.
- Opportunities for future work in optimizing implementation and expanding system functionalities.

2.A decentralized way to store and authenticate educational documents on private blockchain.

[1]Shrivastava, Ajay Kumar, Chetan Vashistth, Akash Rajak, and Arun Kumar Tripathi. "A decentralized way to store and authenticate educational documents on private blockchain." In 2019 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), vol. 1, pp. 1-6. IEEE, 2019.

Abstract:

Implementing a decentralized private Blockchain system for academic document storage and verification streamlines the verification process, enhancing speed and security. Blockchain technology eliminates the need for multiple verification layers and offers real-time auditing, improving efficiency. It secures personal education data and mitigates misuse by requiring private keys and stringent authentication.The proposed system uses a private Blockchain managed by select vendors, employing a proof-of-stake consensus mechanism. Document storage is facilitated through a private IPFS database server. While Ethereum is the primary choice, Hyperledger Fabric is also an option.

Inferences:

- -Decentralized private Blockchain implementation for academic document storage and verification enhances self-sovereignty.
- Significantly reduces time and cost associated with verification across various layers.
- Documents stored on Blockchain are highly secure, accessible only via private keys and proper authentication.

- Proposes a private Blockchain managed by select vendors, utilizing a proof-of-stake consensus mechanism.
- Utilizes a private IPFS database server to store documents within the Blockchain ecosystem.
- Considers Ethereum Blockchain as the primary ecosystem, with the possibility of using Hyperledger Fabric.

3.Nftcert: Nft-based certificates with online payment gateway,

[4]X. Zhao and Y.-W. Si, "Nftcert: Nft-based certificates with online payment gateway,"

in 2021 IEEE International Conference on Blockchain (Blockchain). IEEE, 2021,

pp. 538–543.

Abstract:

This paper addresses the persistence of traditional paper-based academic certificates, which continue to create challenges in terms of verification processes. To overcome these issues, the paper introduces an innovative framework called NFTCert, which is built on the principles of Non-Fungible Tokens (NFTs) and utilizes Blockchain technology to establish a secure connection between a certificate and its rightful owner. The framework's implementation encompasses various aspects, including defining schemas, creating and verifying NFT-based certificates, and facilitating their revocation if necessary. One notable feature of NFTCert is the integration of a payment gateway within the certificate creation process, ensuring a more extensive user base. Unlike many Blockchain systems that rely on cryptocurrencies, this framework enables participants to engage without the need for such digital currencies. Overall, NFTCert is designed to offer usability, authenticity, confidentiality, transparency, and availability, setting it apart from existing Blockchain-based solutions.

Conclusion:

- NFTCert proposes a novel certificate framework based on Non-Fungible Tokens (NFTs).

- NFTs are unique and irreplaceable, making them ideal for ensuring the authenticity of educational certificates.
- The framework addresses concerns about certificate fraud and misuse by creating tamper-proof digital certificates.
- Users can centralize their educational certificates for easy storage and presentation.
- External organizations, like overseas universities and employers, can efficiently verify an individual's educational background by accessing their digital wallet.
- NFTCert prioritizes usability, authentication, confidentiality, transparency, and availability in the context of certificate management and verification.

4.Decentralized Society: Student's Soul Using Soulbound Tokens

[7]U. Tejaswin, S. J. Kennith, R. Manivel, K. C. Shruthi and M. Nirmala, "Decentralized Society: Student's Soul Using Soulbound Tokens," 2023 International Conference for Advancement in Technology (ICONAT), Goa, India, 2023, pp. 1-4, doi: 10.1109/ICONAT57137.2023.10080658.

Abstract:

This paper explores the potential of non-transferable tokens, known as soulbound tokens (SBTs), within the context of web3 and decentralized societies. While web3 primarily emphasizes decentralized financial transactions with transferable tokens, this study delves into the application of SBTs to enhance individual credibility. SBTs encode individuals' affiliations, creating a unique and trustworthy network. The focus is on students' academic achievements and credibility, illustrating how these credentials can be securely stored and verified within a decentralized framework. Compared to centralized systems, this approach promises greater privacy and security, ultimately elevating the credibility of the stored data.

Inferences:

- This paper introduces the concept of non-transferable soulbound tokens (SBTs) in the context of web3 and decentralized societies.
- SBTs are proposed as a means to enhance individual credibility by encoding affiliations and academic achievements.

- The study highlights the advantages of using a decentralized system for storing and verifying academic credentials, emphasizing improved privacy and security.
- SBTs offer an innovative approach to fostering trust within a network, contrasting with the predominant focus on transferable tokens for financial transactions.
- The ultimate goal is to elevate the credibility of data in a decentralized environment.

5.Skillcheck: An incentive-based certification system using blockchains.

Gupta, Jay, and Swaprava Nath. "Skillcheck: An incentive-based certification system using blockchains." In 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), pp. 1-3. IEEE, 2020.

Abstract:

The paper addresses the challenge of skill verification in workforce hiring, highlighting the common difficulty in confirming applicants' skills due to the non-immediate verifiability and cost of testing claimed skills. While existing blockchain-based approaches focus on storing traditional university certificates, the proposed SkillCheck platform introduces a novel solution. SkillCheck not only considers skill certification but also addresses key issues like scalability, uniform grading, and honest effort extraction. It incentivizes grading efforts through token-based payments generated from platform users, such as recruiters and test takers. The paper provides a comprehensive overview of the platform's design and its provable properties, offering a promising solution for efficient and reliable skill verification in a decentralized manner.

Inferences:

- SkillCheck is a blockchain-based certification system addressing certification and evaluation challenges.
- It tackles scalability, fairness, and security issues through innovative incentive mechanisms for evaluators.
- Smart contracts automate payments, ensuring transparency and accountability.
- The platform's design, implementation, and provable properties are comprehensively detailed.

- SkillCheck has the potential to transform certification and evaluation processes, creating new opportunities for individuals and organizations.

2.2 Books and newspapers referred

Articles:

- The benefits of blockchain for digital certificates: A multiple case study analysis. Authors- Shuyi Pu, Jasmine Siu Lee Lam
- Highly private blockchain-based management system for digital COVID-19 certificates. Authors-Rosa Pericàs-Gornals, Macià Mut-Puigserver
- SBT: the Key to Unlock the Future of DeSoc .HTX Research

2.3. Interaction with Domain Experts:

- Comprehensive Portfolio Management: Expand the platform to provide users, whether students or entities, with an integrated and user-friendly portfolio management system. This feature will allow users to conveniently access, view, and organize their Soul Bound NFTs (SBNs) or NFTs in a single location, enhancing user experience and efficiency.

- Ranking and Gamification: Implement a ranking and gamification system to incentivize and reward users for actively engaging with the certification and achievement process. Introduce achievement levels, badges, and leaderboards to recognize and motivate individuals based on their certificate acquisition and participation in the ecosystem.

- Enhanced Certificate Rollup: Incorporate a certificate rollup mechanism that enables users to bundle multiple certificates and achievements into a single, easily shareable entity. This feature streamlines the presentation of accomplishments, making it simpler for users to showcase their skills and qualifications to potential employers or institutions.

- Multi-Batch Transactions: Facilitate the process of issuing certificates and achievements through multi-batch transactions. This enhancement will save time and reduce transaction costs when generating multiple SBNs or NFTs simultaneously. It streamlines the administrative aspects of certificate issuance.

- User Feedback and Continuous Improvement: Establish a feedback loop for users to provide input on the platform's functionality and features. Regularly update the application based on user suggestions to ensure it remains relevant and aligned with user needs and expectations.

- Integration with Educational Institutions: Collaborate with educational institutions and organizations to seamlessly integrate the platform with their existing systems. This will facilitate the automatic generation of certificates and achievements, streamlining the certification process.

- Expansion to Other Credentials: Extend the platform's capabilities beyond certificates and achievements to cover a broader spectrum of digital credentials, such as licenses, diplomas, and other proofs of qualifications. This expansion will diversify the use cases and user base of the platform.

- Community Building and Partnerships: Foster a vibrant user community and explore strategic partnerships with institutions, employers, and other stakeholders. These collaborations can contribute to the platform's growth and acceptance within the academic and professional ecosystem.

Chapter 3: Requirements

3.1 Proposed model

The proposed model of DeCat is designed to provide a secure, decentralized, and scalable solution for the issuance and verification of digital achievements and credentials. The model consists of several key components:

1. Identity Verification:

- Issuers go through a robust identity verification process using login credentials or third-party verification (e.g., Worldcoin).
- Verification ensures that only legitimate entities have the authority to mint Soul Bound Tokens (SBTs).

2. Smart Contract Architecture:

- Utilizes a modified ERC721 standard for SBTs, incorporating unique features inspired by Soul Bound Tokens.
- The smart contract logic ensures that once an SBT is minted to an address, it becomes non-transferable and non-burnable, ensuring a permanent link between the token and the user.

3. Issuer Dashboard:

- Features a user-friendly dashboard accessible only to verified issuers.
- Issuers can input details about the SBT, including metadata, achievements, and other relevant information.
- Supports the import of a CSV dataset for efficient, bulk transactions to multiple recipients.

4. Bulk Transaction Functionality:

- Allows issuers to send SBTs to multiple recipients in a single, bulk transaction.
- Enhances scalability and practicality, especially in scenarios where issuers need to distribute certificates to a large number of recipients.

5. Legitimacy Check:

- Recipients can showcase their SBTs to anyone as proof of their achievements.
- The unique identifier of each token enables easy verification of its legitimacy by checking its origin and confirming its validity on the blockchain.

3.2 Functional Requirements

1. User Authentication and Identity Verification:

- Requirement: Users must be able to authenticate themselves securely.
- Details: The system should implement a robust user authentication mechanism, and for issuers, there should be an identity verification process using either login credentials or a third-party service like Worldcoin.

2. Issuer Dashboard:

- Requirement: Issuers should have a dedicated dashboard.
- Details: The dashboard must allow issuers to input details about the Soul Bound Tokens (SBTs), including metadata, achievements, and other relevant information. It should also support importing a CSV dataset for efficient bulk transactions.

3. SBT Minting:

- Requirement: Issuers should be able to mint SBTs.
- Details: Issuers, upon successful verification, should be able to create SBTs by entering relevant details. The SBTs must adhere to a modified ERC721 standard that makes them non-transferable and non-burnable.

4. Bulk Transaction Functionality:

- Requirement: Issuers should be able to send SBTs in bulk to multiple recipients.
- Details: The system must support bulk transactions to efficiently send SBTs to a large number of recipients in a single transaction.

5. Legitimacy Check:

- Requirement: Recipients and verifiers should be able to check the legitimacy of SBTs.
- Details: Each SBT should have a unique identifier, and the system must provide a mechanism for anyone to verify the legitimacy of a token by checking its origin and confirming its validity on the blockchain.

6. Ethereum Testnet Integration:

- Requirement: The Dapp should be built on the Ethereum testnet (Sepholia).
- Details: Development and testing should be conducted on the specified Ethereum testnet to ensure compatibility and performance.

7. Scalability Measures:

- Requirement: The system should handle scalability effectively.
- Details: The Dapp must implement multi-batch transactions and rollup mechanisms to efficiently scale the application as the user base grows.

8. User Interface (UI):

- Requirement: User interfaces must be intuitive and user-friendly.
- Details: Both issuers and recipients should have interfaces that are easy to navigate, providing a positive user experience.

9. Security Measures:

- Requirement: The system must prioritize security.
- Details: Security features should include secure user authentication, protection of private keys, regular smart contract audits, and measures to safeguard user data.

10. Documentation:

- Requirement: Comprehensive documentation should be available.
- Details: The system must have clear and accessible documentation for users, including issuers, recipients, and developers. This should cover how to use the Dapp, security practices, and troubleshooting.

3.3.Non-Functional Requirements

- Scalability: The platform should be designed to handle large numbers of users, music tracks, and transactions. It should be able to scale up or down as needed to meet demand.
- Security: The platform should be built with robust security measures to prevent hacking, fraud, and other cyber threats. It should also protect user data privacy.
- Reliability: The platform should be highly reliable, with minimal downtime and fast response times.
- Interoperability: The platform should be interoperable with other blockchain-based systems and music streaming platforms, allowing for seamless integration and data sharing.
- Usability: The platform should be easy to use and intuitive, with a user-friendly interface that allows users to navigate the system and perform tasks without difficulty.
- Performance: The platform should perform well, with fast load times and minimal latency when streaming music tracks.
- Compliance: The platform should comply with relevant legal and regulatory requirements, such as copyright laws and anti-money laundering regulations.
- Transparency: The platform should be transparent in its operations, with clear documentation and reporting of all transactions and activities.
- Availability: The platform should be available 24/7, with minimal downtime or service interruptions.
- Sustainability: The platform should be designed with sustainability in mind, minimizing energy consumption and carbon emissions.

3.4.Hardware & Software Requirements

Hardware :

Server Infrastructure:Processor: Multi-core processor (e.g., Intel Xeon, AMD Ryzen)

- RAM: 16 GB or higher
- Storage: SSD for faster data access (minimum 256 GB)
- Network: High-speed internet connection

Blockchain Node:

- Processor: Multi-core processor
- RAM: 16 GB or higher
- Storage: SSD with ample storage space (500 GB or more)
- Network: High-speed internet connection

Load Balancer (for scalability):

- Processor: Multi-core processor
- RAM: 8 GB or higher
- Network: High-speed internet connection

Development and Testing Machines:

- Processor: Dual-core or higher
- RAM: 8 GB or higher
- Storage: SSD for faster development and testing

Software :

Operating System:

- Server: Linux-based OS (e.g., Ubuntu Server)
- Development Machines: Windows, macOS, or Linux

Blockchain Software:

- Ethereum Node: Geth or Parity for Ethereum blockchain
- Smart Contract Development: Solidity programming language
- Web3 Libraries: Web3.js or ethers.js
- Tools : WorldCoin , OpenSea

Backend Framework:

- Node.js: For server-side JavaScript runtime
- Express.js: Web application framework for Node.js

Frontend Framework:

- React.js : For building dynamic user interfaces

Smart Contract Deployment and Testing:

- Truffle or Hardhat: Frameworks for deploying and testing smart contracts

Version Control:

- Git: For version control and collaborative development

3.5.Technology and Tools utilized

Ethereum Blockchain: The primary blockchain for deploying smart contracts.

Solidity: A programming language for writing smart contracts on the Ethereum platform.

Truffle Suite: Development environment, testing framework, and asset pipeline for Ethereum.

Web3.js: A JavaScript library for interacting with the Ethereum blockchain.

Backend Development:

Node.js: JavaScript runtime for server-side development.
Express.js: Web application framework for Node.js.

Frontend Development:

React.js: JavaScript library for building user interfaces.

Smart Contract Deployment:

Ganache:A personal blockchain for Ethereum development.

Testing:

Mocha and Chai: Testing frameworks for JavaScript and Solidity.
Jest: JavaScript testing framework for React applications.

Version Control:

Git: Distributed version control system.

3.6.Constraints of working

Blockchain Scalability:

- Description: Blockchain networks, including Ethereum, may face scalability issues, leading to delays in transaction processing and higher fees during periods of network congestion.
- Mitigation: Utilize scaling solutions, such as layer-2 solutions like rollups, to enhance the scalability of the application.

Smart Contract Security:

- Description: Smart contracts are susceptible to vulnerabilities, and security audits are crucial to identifying and addressing potential issues.
- Mitigation: Regularly audit smart contracts using tools like MythX and engage with professional auditing services.

Ethereum Gas Fees:

- Description: Transaction fees (gas fees) on the Ethereum network can be unpredictable and may become expensive during periods of high demand.
- Mitigation: Consider implementing gas optimization strategies and explore alternative blockchains or layer-2 solutions to mitigate high gas fees.

Regulatory Compliance:

- Description: Blockchain and cryptocurrency projects may face evolving regulatory landscapes, leading to legal uncertainties.

- Mitigation: Stay informed about regulatory developments, collaborate with legal experts, and design the system with compliance in mind.

Third-Party Dependencies:

- Description: Reliance on third-party services or tools may introduce dependencies that are beyond the project team's control.
- Mitigation: Choose reputable and well-supported third-party services, have contingency plans for potential service disruptions, and consider decentralized alternatives where possible.

Chapter 4: Proposed Design

4.1 Block Diagram of the proposed system

The block diagram encompasses a comprehensive process that empowers institutes to provide students with SoulBound Tokens, acting as certificates, to authenticate their newly acquired skills and workshop attendance. This process unfolds within the confines of our dedicated platform, ensuring a secure and streamlined approach to certification.

1. Authorized Personnel Access:

The process commences with authorized institute personnel accessing our platform. These personnel are entrusted with login credentials, which serve as their gateway to initiate the certification process.

2. Certificate Template Creation:

Within the platform, authorized personnel can design the certificate template. They have the flexibility to provide the certificate's visual identity by uploading an image, along with specifying its name and description. This template will serve as the foundation for all issued certificates.

3. Student Data Input:

The institute personnel input student details, such as wallet addresses and names, using a CSV file. This data is vital for personalizing the certificates and associating them with the respective students.

4. Bulk Minting with Roll-Up Mechanism:

One of the key features of our system is the implementation of a Roll-up mechanism. This mechanism enables the consolidation of multiple certificate minting transactions into a single, efficient transaction. By doing so, it not only saves time but also reduces gas fees, enhancing the overall system efficiency.

5. Personnel Validation:

The institute personnel play a crucial role in ensuring the legitimacy of participants. They validate and cross-reference the provided student data to confirm the authenticity of those receiving certificates. This step adds an extra layer of trust and security to the certification process.

6. SoulBound Token Issuance:

As a result of the combined efforts of the authorized personnel and the Roll-up mechanism, unique SoulBound Tokens (certificates) are issued to students. These tokens are securely stored in their respective wallet addresses, symbolizing the students' achievements and workshop attendance.

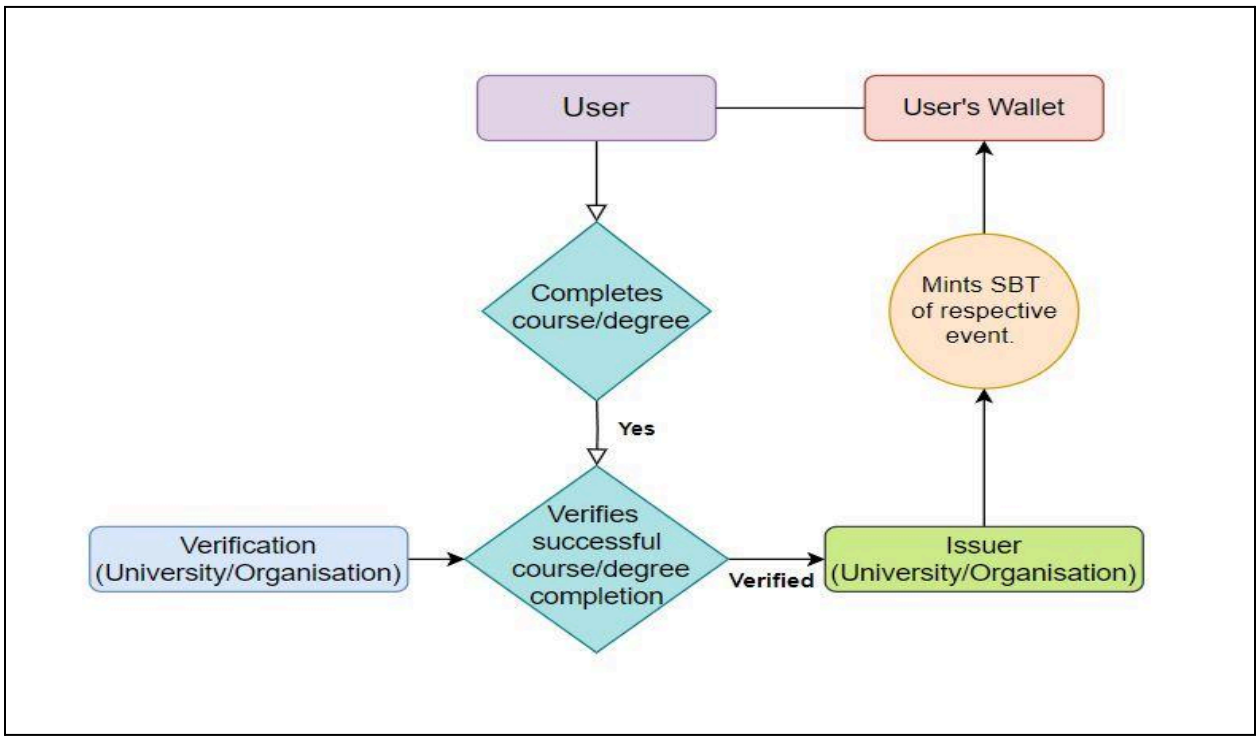

Fig.1. Block Diagram

4.2 Modular diagram

1. Certificate(SBT) Creation:

   The initiation of the certificate template creation process commences when an accredited institutional entity, acting as the issuer, submits essential components comprising the certificate image, name, and description. These pivotal elements are employed in the formation of the fundamental framework for generating certificates. The orchestration of this pivotal step is executed through the secure and authenticated access to the dedicated platform, a prerogative exclusively granted to duly authorized institutional entities.

   In this highly-regulated and meticulously orchestrated process, the issuer's login credentials serve as the gateway to embark on the journey of transferring certificates. The act of furnishing the certificate image, along with its designated name and descriptive particulars, is the initial architectural phase towards fashioning a certificate template.

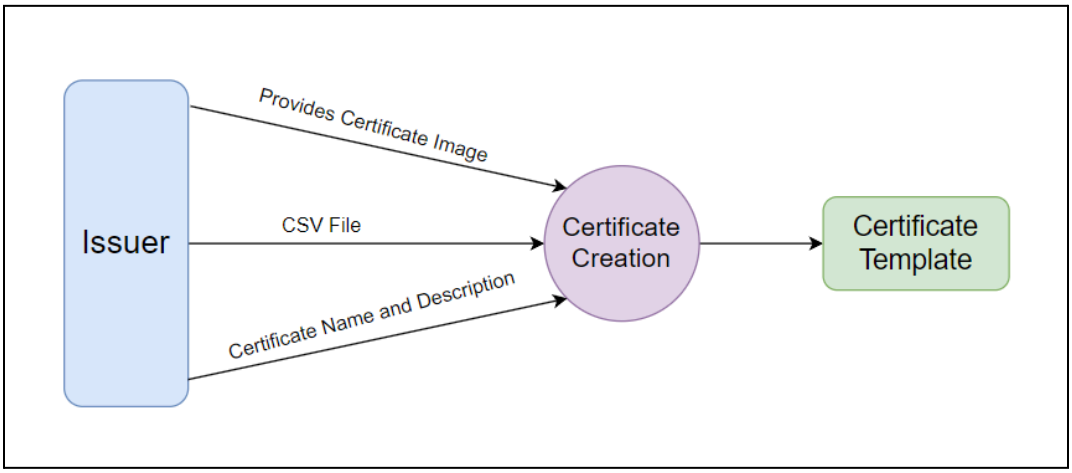

Fig.2. Certificate Creation

2. SBT Minting :

   The template established above serves as the blueprint for the creation of distinct SoulBound Tokens (certificates). These tokens are meticulously crafted by importing data from a CSV file that is securely provided by the authorized issuer. Through this data integration process, each certificate assumes its unique identity, encapsulating the achievements and credentials of the recipients, thus reinforcing the unassailable and singular nature of the SoulBound Tokens.

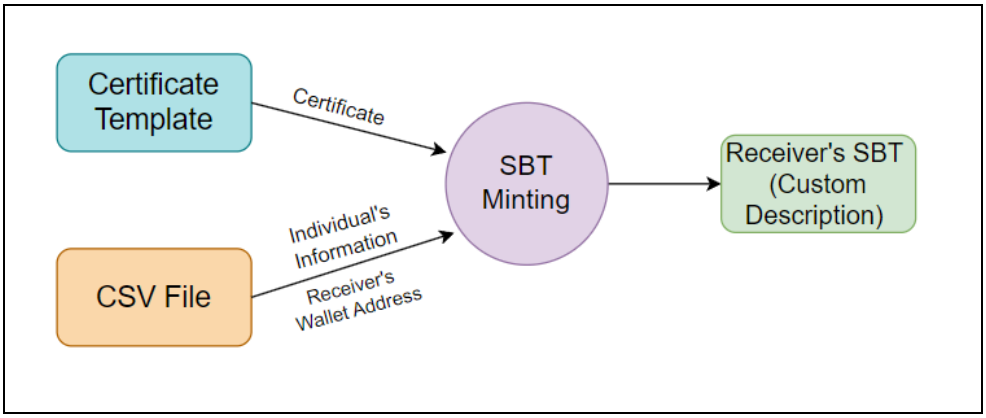

Fig.3. SBT Minting

3. Roll-Up Mechanisms: In our continuous pursuit to optimize the scalability and efficiency of our blockchain application, we've incorporated a roll-up mechanism into our system. This forward-looking approach represents a significant leap in the evolution of blockchain technology. By harnessing the capabilities of roll-ups, we can unlock the ability to dramatically reduce the duration of transactions while simultaneously curbing the financial overhead associated with gas fees.

   Roll-up technology achieves this by ingeniously consolidating numerous individual transactions into a single, comprehensive transaction, thereby streamlining the data processing and execution process on the blockchain. As a result, our application benefits from a more agile and cost-effective workflow. This advancement is not only a testament to our commitment to sustainability and cost-efficiency but also an affirmation of our dedication to providing users with an exceptional experience.

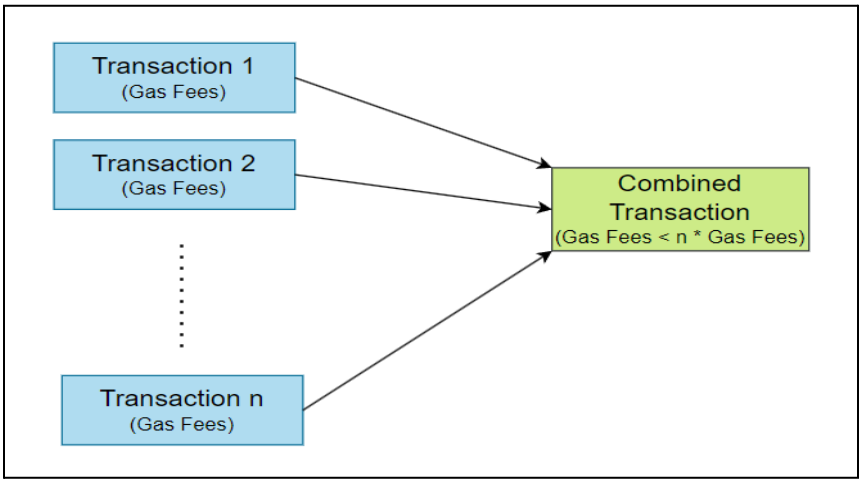

Fig.4. Roll-Up Mechanism

4.3 Detailed Design

Our system design represents a multifaceted approach to revolutionize the certification process, with the integration of a roll-up mechanism, advanced API functionality, and gamification elements. This comprehensive system is specifically designed for universities and organizations to efficiently issue certificates and promote education with incentives, all while optimizing the scalability of the underlying blockchain.

1. Roll-Up Mechanism Integration:

At the core of our system, we have seamlessly integrated a roll-up mechanism into a public blockchain, which has undergone rigorous testing to ensure its robustness and reliability. This mechanism operates as a layer 2 scaling solution, optimizing the transaction process. By aggregating multiple transactions into a single batch, we significantly reduce transaction times and lower associated costs. This not only enhances the blockchain's scalability but also makes it more user-friendly by reducing gas fees. As a result, universities and organizations can process certificate-related transactions more efficiently, providing a streamlined experience for both certificate issuers and recipients.

2. Streamlined Certificate Issuance:

Our system allows authorized personnel from universities and organizations to easily input certificate details by importing CSV files. This includes certificate template information, such as images, names, and descriptions. The user-friendly interface ensures a seamless and efficient process. These details are used to create customized certificates that are securely issued as SoulBound Tokens, providing a trustworthy testament of achievements and skills to students.

3. API Integration for Enhanced Functionality:

Our system is designed to be highly extensible and adaptable. It leverages APIs to increase its functionality and integration capabilities. These APIs enable seamless connections with various services and platforms, enhancing the overall user experience. For instance, APIs can be used to link with existing university databases, external verification services, or blockchain networks, further expanding the system's capabilities and utility.

4. Gamification for Education Promotion:

To encourage active participation and motivate students, we have introduced gamification elements into our system. Students are ranked on a leaderboard based on their certificate achievements. This competitive aspect fosters a sense of achievement and incentivizes further learning and participation. Top performers receive rewards, which can include digital tokens, premium content access, or other enticing incentives. The gamification twist not only celebrates accomplishments but also promotes a culture of continuous learning.

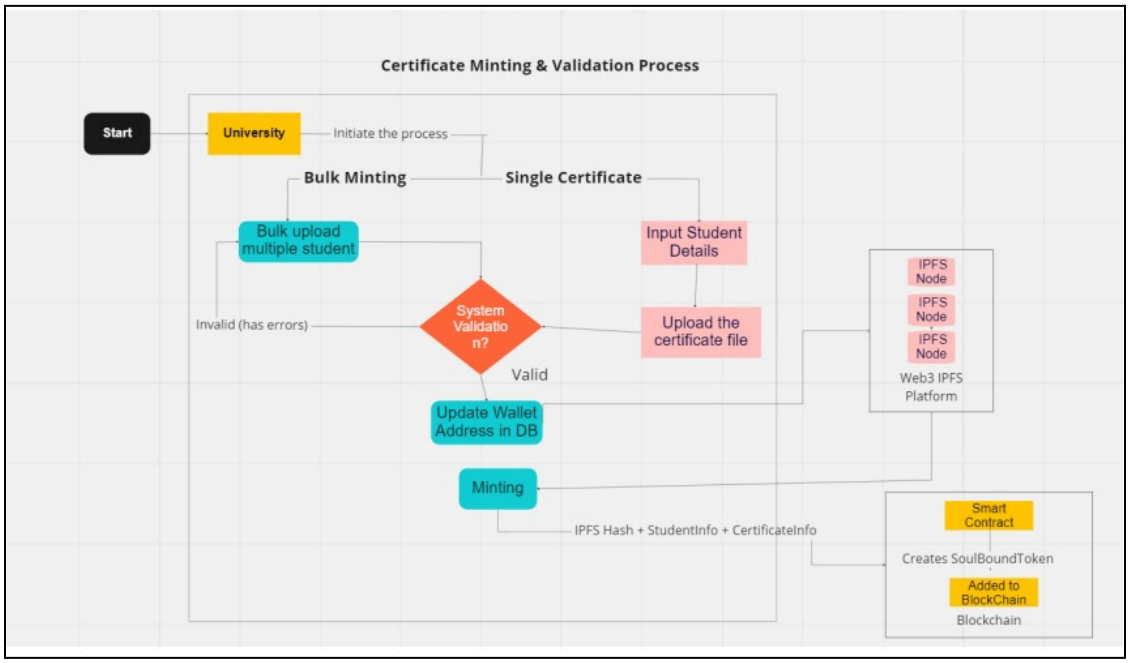

Fig.5. Detailed System Design

4.3 Implementation Screenshots

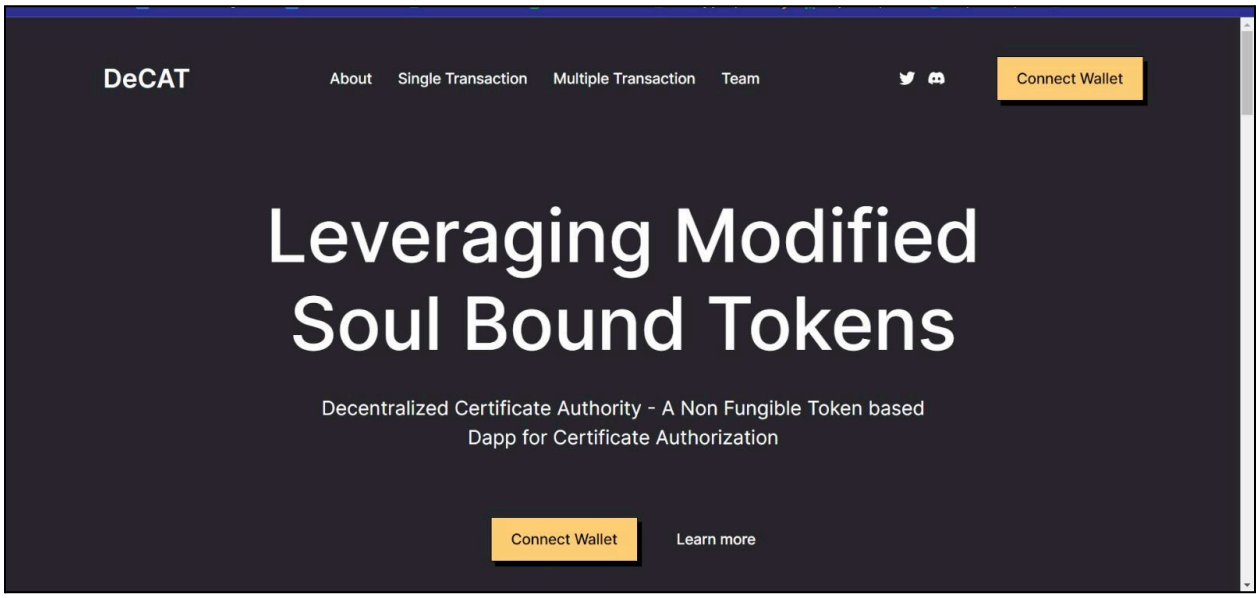

Fig.6. Landing Page (Frontend)

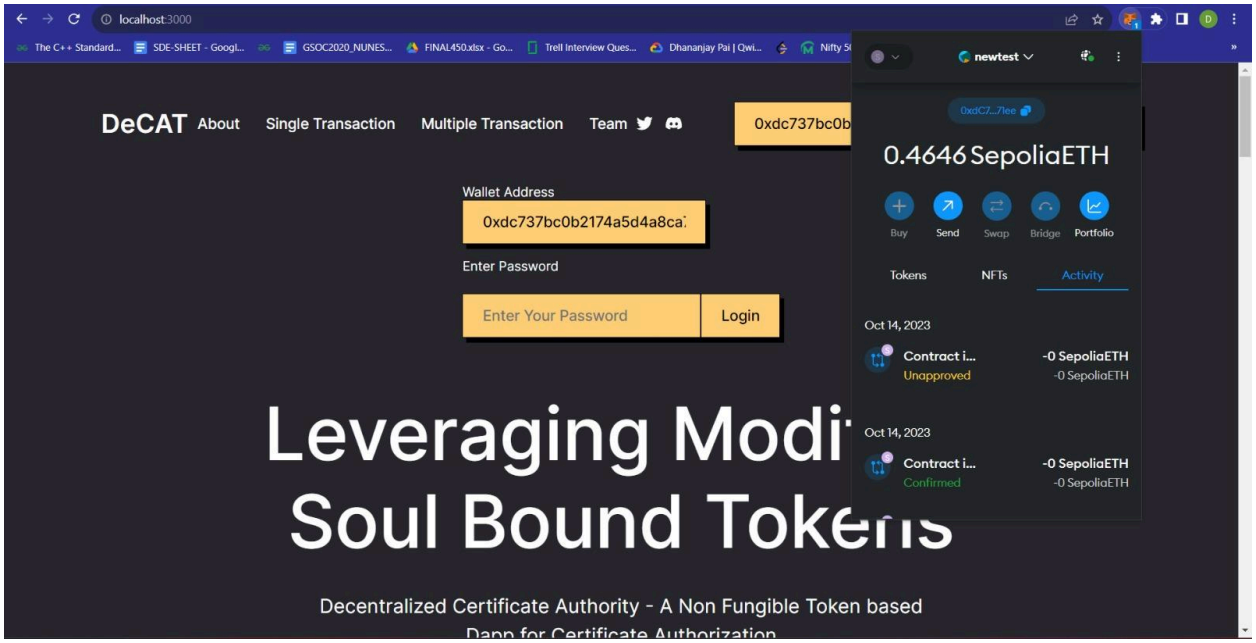

Fig.7. Wallet Connection and Login

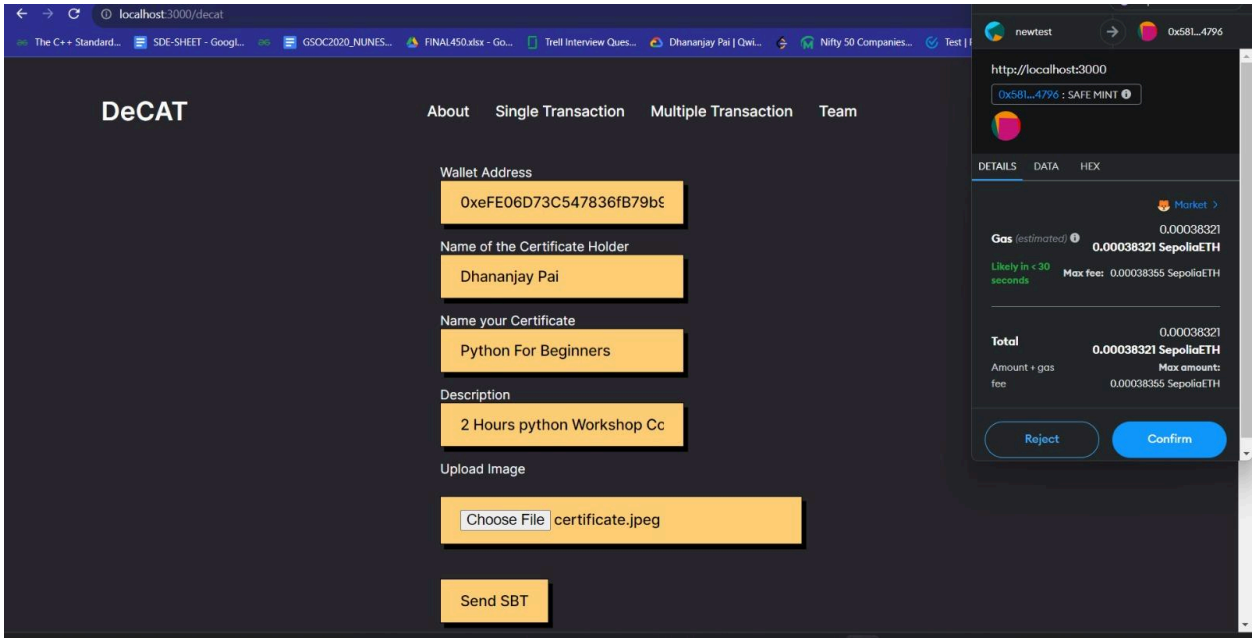

Fig.8. Single Batch Transaction.

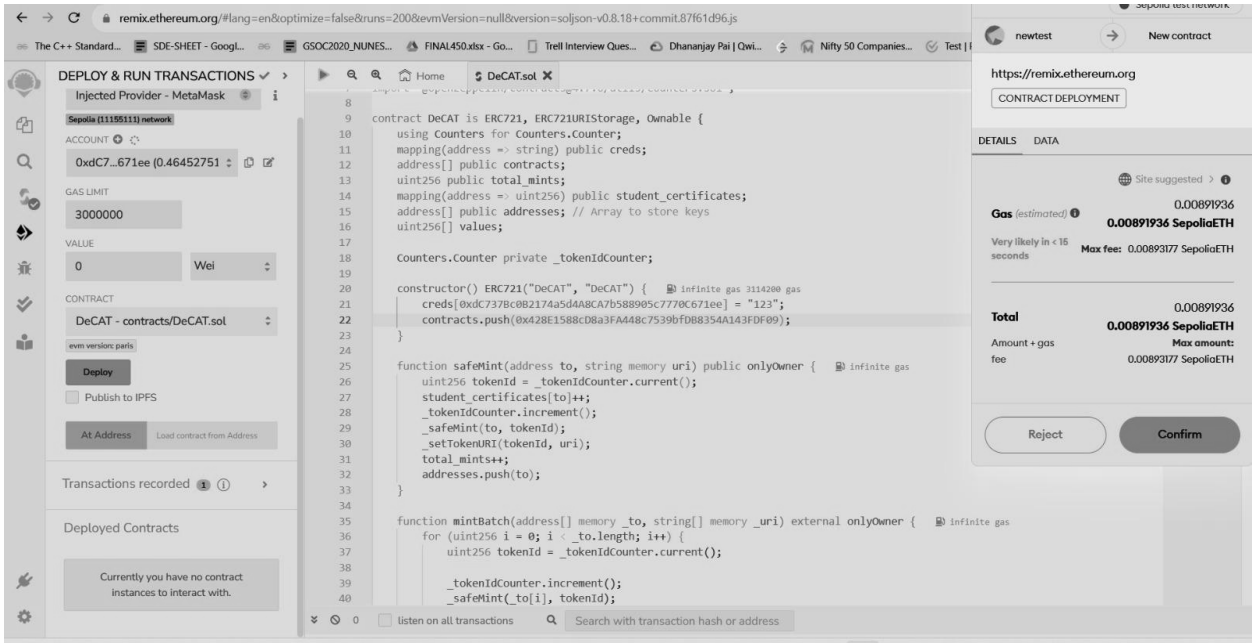

Fig.9. Smart Contract Deployment

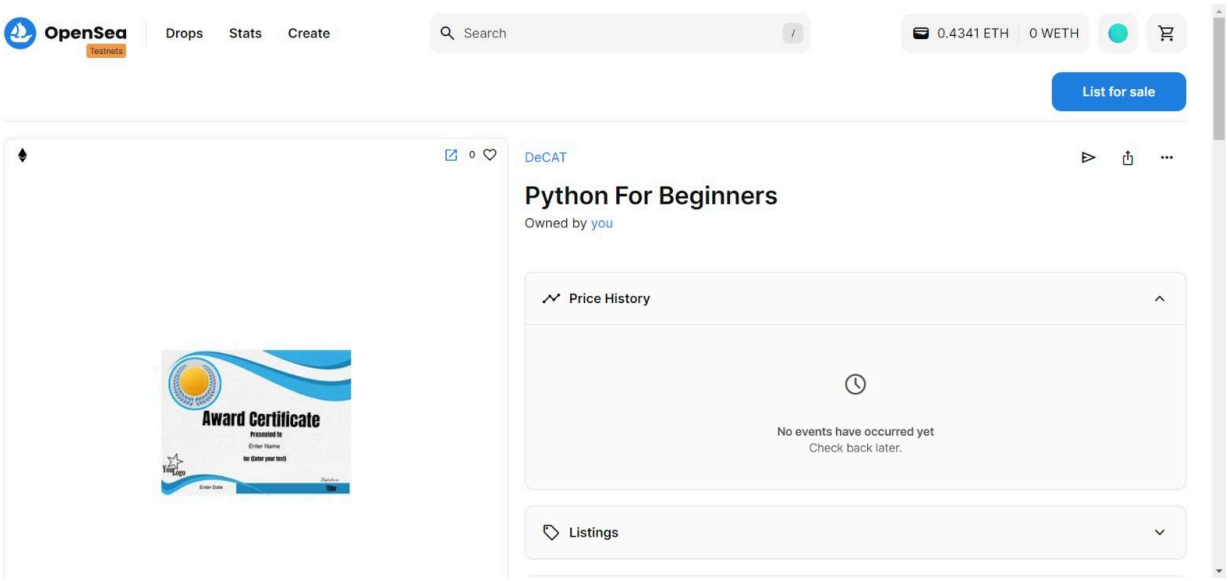

Fig.9.SBT sent to the wallet address given

5. Results and Discussions

The implementation of DeCat has yielded notable results, marking a transformative journey in the realm of digital credentialing. The project's outcomes and subsequent discussions can be summarized across key dimensions:

1. Authentication and Identity Security:

- Results: The introduction of robust issuer verification mechanisms, using login credentials or third-party services like Worldcoin, has fortified the platform's security.
- Discussion: Establishing a secure authentication process ensures that only legitimate issuers gain access to the system, mitigating the risk of unauthorized minting.

2. Immutability with Soul Bound Tokens (SBTs):

- Results: The modification of the ERC721 standard to create SBTs has successfully anchored achievements to users' digital identities, providing an immutable representation of their accomplishments.
- Discussion: SBTs, being non-transferable and non-burnable, guarantee the permanent association of achievements with the user, addressing the challenge of credentials being easily duplicated.

3. Bulk Transaction Functionality:

- Results: The incorporation of bulk transaction functionality, enabled by importing CSV datasets, has streamlined the process of distributing SBTs to multiple recipients in a single transaction.
- Discussion: This feature enhances the efficiency of the platform, particularly in scenarios where issuers need to distribute certificates to a large number of recipients.

4. Legitimacy Verification:

- Results: Recipients can confidently showcase their SBTs as a portfolio of achievements. The transparency of blockchain allows easy verification of token legitimacy by checking the token's origin.
- Discussion: This capability not only empowers individuals to demonstrate their accomplishments but also provides a trust layer by allowing others to independently verify the legitimacy of presented credentials.

5. Scalability Measures:

- Results: The project outlines plans for future scalability with the incorporation of multi-batch transactions and rollup mechanisms.
- Discussion: This forward-looking approach acknowledges the importance of scalability in handling increased user transactions and positions the project for sustained growth.

6. User-Friendly Dashboard:

- Results: Issuers benefit from an intuitive dashboard that facilitates the entry of SBT details and achievements, contributing to the overall usability of the platform.
- Discussion: A user-friendly interface enhances the adoption of the platform, ensuring that issuers can efficiently contribute to the creation and distribution of SBTs.

6. Plan of action for the next semester

1. Integrating the functionality of customizable SoulBound Token using the csv dataset.
2. Integrating the Gamification model to increase interaction and promote education.
3. Improving the user experience of the platform.

7. Conclusions

The project's significance lies not merely in its technological innovations but in its profound impact on trust within the digital realm. By anchoring achievements to individual digital identities, SBTs serve as verifiable and tamper-proof representations of one's accomplishments. The integration of issuer verification, bulk transaction functionality, and plans for scalability enhancements positions this Dapp at the forefront of secure digital credential management.

The user-friendly dashboard empowers issuers to contribute to the integrity of the system, allowing them to input SBT details and achievements efficiently. Bulk transactions, facilitated by CSV datasets, redefine the efficiency of distributing SBTs to multiple recipients.

As recipients showcase their SBTs, a new era of transparency and trust is ushered in. Anyone can easily verify the legitimacy of a token by tracing its origin on the blockchain, reinforcing the value of authentic accomplishments.

Looking forward, the project's commitment to scalability with planned multi-batch transactions and rollup mechanisms ensures its adaptability to the evolving needs of a growing user base. It is not just a solution for today but a dynamic platform designed to withstand the challenges of tomorrow.

In summary, Decat goes beyond the usual limits of digital credentialing. It represents a promise to prioritize trust, transparency, and security in the constantly growing digital world. When we look back at this project, we see how it's more than just meeting a requirement – it's changing the way we think about authenticity in the digital era. The Soul Bound Tokens Dapp is like a guiding light for innovation, leading us toward a future where accomplishments aren't just shown but also protected, taking digital trust to new levels

8. References

Research Papers referred/ Journals/ Articles referred

[1]Shrivastava, Ajay Kumar, Chetan Vashistth, Akash Rajak, and Arun Kumar Tripathi. "A decentralized way to store and authenticate educational documents on private blockchain." In 2019 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), vol. 1, pp. 1-6. IEEE, 2019.

[2]Cheng, Jiin-Chiou, Narn-Yih Lee, Chien Chi, and Yi-Hua Chen. "Blockchain and smart contract for digital certificate." In 2018 IEEE international conference on applied system invention (ICASI), pp. 1046-1051. IEEE, 2018.

[3]N. Buchmann, C. Rathgeb, H. Baier, C. Busch, and M. Margraf, “Enhancing breeder document long-term security using blockchain technology,” in 2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC), vol. 2. IEEE, 2017, pp. 744–748.

[4]X. Zhao and Y.-W. Si, “Nftcert: Nft-based certificates with online payment gateway,” in 2021 IEEE International Conference on Blockchain (Blockchain). IEEE, 2021,

pp. 538–543.

[5]E. G. Weyl, P. Ohlhaver, and V. Buterin, “Decentralized society: Finding web3’s soul,” Available at SSRN 4105763, 2022.

[6]Ansori, Muhammad Rasyid Redha, Revin Naufal Alief, Ikechi Saviour Igboanusi, Jae Min Lee, and Dong-Seong Kim. "Batch Minting-enabled Digital Certificates Based on Soulbound Token for Achievement Verification." 한국통신학회 학술대회논문집 (2023): 1350-1351.

[7]U. Tejaswin, S. J. Kennith, R. Manivel, K. C. Shruthi and M. Nirmala, "Decentralized Society: Student’s Soul Using Soulbound Tokens," 2023 International Conference for Advancement in Technology (ICONAT), Goa, India, 2023, pp. 1-4, doi: 10.1109/ICONAT57137.2023.10080658.

[8]Gupta, Jay, and Swaprava Nath. "Skillcheck: An incentive-based certification system using blockchains." In 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), pp. 1-3. IEEE, 2020.

[9]Dalal, Jignasha, Meenal Chaturvedi, Himani Gandre, and Sanjana Thombare. "Verification of identity and educational certificates of students using biometric and blockchain." In Proceedings of the 3rd International Conference on Advances in Science & Technology (ICAST). 2020.

[10]Billah, Sifat Nur, Rehana Pollobe, Farjana Hossain, Nahid Murad Abir, Afsana Zaman Zarin, and M. F. Mridha. "Blockchain Based Architecture for Certificate Authentication." In Proceedings of the International Conference on Innovative Computing & Communication (ICICC). 2021.

9. Appendix

a. List of Figures

Figure Number	Heading	Page no.
1	Block Diagram	28
2	Certificate Creation	29
3	SBT Minting	30
4	Roll-Up Mechanism	30
5	Detailed System Design	32
6	Landing Page	33
7	Wallet Connection	33
8	Single Batch	34
9	Smart Contract	34
10	SBT showcase	35