IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Synergy: Decentralized Certificate Verification And Validation

[1]Mr. Kumar K, [2]Gopala Krishna V, [3]Akshay Vivekananda B, [4]Arjun Bharadwaj, [5]Vaibhav Nayak

[1]Assocoate Professor, [2]Student, [3]Student, [4]Student, [5]Student

[1]Department of Computer Science and Engineering,

[1]K S Institute of Technology, Affiliated to VTU, Bangalore, India

Abstract: This project introduces a blockchain-based e-vault system that ensures secure, transparent, and tamper-proof storage and verification of digital certificates. By utilizing the immutable and decentralized nature of blockchain technology, the system effectively eliminates risks associated with certificate fraud and unauthorized alterations. It features two types of users: Admin/Authorized Users, who can upload certificates with recipient details, and Normal Users, who are permitted to verify them. Upon successful upload, certificates are stored on the blockchain and recipients are notified via email with the certificate ID and related information. Users can access all their certificates through email-based login, with an optional Merge Account feature to combine multiple accounts for unified access. Additional functionalities include a Portfolio Page for resume generation, a dynamic pricing model to support institutional sustainability, a user guidance feature for easier navigation, and a live chatbot for real-time assistance. This system not only secures digital credentials but also empowers users and organizations with tools for professional development and efficient certificate management.

Keywords: Blockchain, Digital Certificates, E-Vault, Tamper-Proof Storage, Authentication, Certificate Verification, Immutable Ledger, Credential Management, Email-Based Access, Resume Generation, Portfolio Page, Real-Time Support.

I. INTRODUCTION

The rising incidence of certificate forgery and the necessity of secure verification mechanisms have driven the demand for safe, tamper-resistant digital storage solutions. Manual verification processes are usually cumbersome, time-consuming, and vulnerable to forgery, which makes it challenging for employers, schools, and organizations to confirm the genuineness of credentials effectively. An e-vault system based on blockchain technology offers a new solution to these issues by ensuring secure, transparent, and decentralized certificate verification.

This system takes advantage of blockchain technology to secure and store certificates in an irreversible ledger, where once a certificate is uploaded, it cannot be edited or hacked. The site has two roles of users: Admin/Auth Users, who have the power to upload certificates, and Normal Users, who are only allowed to verify them. When an Admin imports a certificate, recipient information in the form of an email ID is given, and on a successful import, an email message with the Certificate ID and related information is notified to the recipient.

For added convenience, users can log in via their registered email and see all related certificates saved in the system. The Merge Account also enhances convenience by enabling users to connect multiple email addresses, combining certificates coming from various sources into one interface. This provides a smooth experience, particularly for individuals who have been certified in several organizations or institutions.

A business-oriented model of pricing has been included in order to achieve sustainability along with serving various needs of users. This model enables organizations, educational institutions, and certification agencies to effectively use the platform while remaining cost-effective. Moreover, a guiding feature has been implemented in order to assist users in easy navigation of the platform, ensuring ease of use. By integrating blockchain security, decentralized certificate storage, and additional career-advancing tools, this e-vault system provides a powerful, efficient, and future-proof solution for certificate management. The platform not only streamlines verification processes but also enables users with tools to showcase their credentials effectively while ensuring trust and authenticity in the digital credentialing ecosystem.

II. LITERATURE REVIEW

"Blockchain Technology for Secure Document Management and Verification" This study [1] explores the application of blockchain in secure document management, emphasizing its ability to prevent tampering and unauthorized modifications. By leveraging a decentralized ledger, the system ensures immutability and transparency, making it a reliable solution for certificate verification. The e-vault platform incorporates these principles to provide secure, verifiable, and easily accessible certificates for users and organizations.

"Enhancing Digital Credential Authentication Using Blockchain" This study [2] highlights the benefits of blockchain in authenticating digital credentials, focusing on its role in reducing fraud and ensuring data integrity. The research discusses the use of smart contracts and cryptographic hashing to maintain authenticity. These concepts are applied in the e-vault system to create a tamper-proof environment where certificates remain verifiable throughout their lifecycle.

"The Impact of Decentralized Identity Management on User Privacy and Security" This study [3] examines how decentralized identity solutions improve security by eliminating central points of failure. The research suggests that users gain greater control over their credentials while ensuring protection from cyber threats. The e-vault system integrates decentralized identity mechanisms, allowing users to access and merge multiple accounts securely without compromising privacy.

"Improving Resume Verification Through Blockchain- Based Credentialing Systems" This study [4] analyses how blockchain enhances resume verification, ensuring that credentials are genuine and unaltered. The research highlights automated resume generation based on verified documents, reducing discrepancies between claims and actual qualifications.

"User Experience and Accessibility in Digital Certificate Management Systems" This study [5] investigates the usability challenges of digital credential management platforms, focusing on navigation, accessibility, and performance. Findings suggest that implementing guided user support and automated assistance improves engagement and adoption. The e-vault system addresses these concerns by incorporating a guiding feature and live chatbot, ensuring users can navigate and utilize the platform effectively.

"Email-Based Notification Systems for Digital Credential Distribution" This study [6] examines the role of automated email notifications in digital credential management, emphasizing their impact on user engagement, timely access, and security. The research highlights how real-time email alerts improve the verification process by providing instant updates to recipients. The e-vault system integrates this approach by sending email notifications upon certificate upload, ensuring that users receive certificate details and authentication information without delay.

III. SOFTWARE REQUIREMENTS

BLOCKCHAIN

A. Solidity

Used to develop the smart contract in the Synergy project. Solidity is the most widely used language to develop smart contracts on the Ethereum blockchain to provide secure execution of transactions and data management.

B. ThirdWeb0

Used to deploy the smart contract on the blockchain. Thirdweb makes it easy to deploy and manage smart contracts, making it possible for the Synergy platform to be incorporated smoothly into blockchain technology.

C. Metamask

A digital wallet used for making transactions on the Ethereum blockchain. MetaMask allows users to interact with the Synergy platform, providing secure management of cryptocurrency and digital assets.

D. Sepolia-ETH

A testnet token for testing blockchain transactions prior to deploying them to the main Ethereum network. Sepolia enables the Synergy platform to test smart contracts and transactions safely and at a reduced cost.

BACKEND

A. Express.Js

A framework built on Node.js for developing the backend of the Synergy platform. Express.js enables the creation of RESTful APIs, handling user requests, routing, and managing data between the frontend and backend.

B. MongoDB

A NoSQL database used to store and manage user data, certificate information, and transaction records. MongoDB provides a flexible, scalable solution for managing unstructured data, which is vital for the dynamic nature of Synergy.

C. Pinata

A cloud storage platform within Synergy to securely hold documents and digital assets. Pinata enables storing files in a decentralized way, providing reliability and scalability for the content of the platform.

D. Email.Js

For sending and receiving emails inside the Synergy platform. Email.js provides security and efficiency to ensure users get transaction notifications, certificate information, and other important data.

FRONTEND

A. Next.Js

A React-based framework that enables client- side and server-side rendering for optimal performance and SEO. Next.js enhances the Synergy platform's speed and user experience by providing fast page loads and seamless interactions.

B. Tailwind CSS

A utility-first CSS framework used to style the Synergy project’s user interface. Tailwind CSS simplifies the styling process, ensuring a clean, responsive, and adaptable design across various devices.

C. UI Libraries

UI libraries such as Ant-D, Shadcn, and DaisyUI are utilized to create UI elements that improve the aesthetic value and user interface of the Synergy platform. Libraries offer pre-built elements and design systems for efficient development.

INTEGRATIONS:

A. Stripe

Payment gateway integrated in the Synergy platform to manage secure payments for services. Stripe enables users to pay for premium features, subscription plans, or other services offered by Synergy.

B. Crisp

24/7 live chat customer support integrated directly into the platform. Crisp allows real-time communication between customer support teams and customers, improved customer satisfaction, and support as and when it is required.

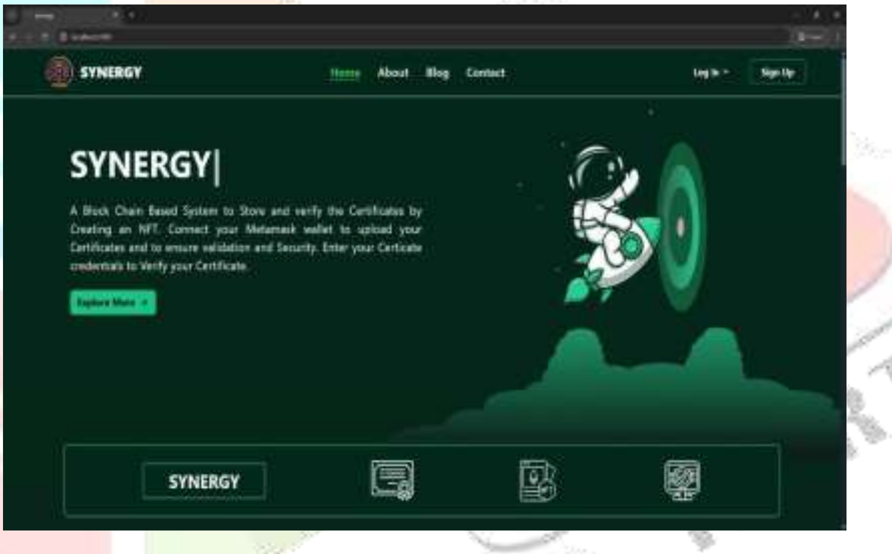
IV. SYSTEM DESIGN

1. User Interface (Frontend)

- ✓ Frontend Framework: The frontend is developed with Next.js, which offers server-side rendering and performance optimization for quick loading as shown in Figure 1.

- ✓ Styling: Tailwind CSS is employed to create a responsive and contemporary user interface that responds to various screen sizes.

- ✓ UI Libraries: Ant-D, Shadcn, and DaisyUI libraries assist in creating dynamic UI elements such as forms, buttons, modals, and tables for certificate handling.



A Block Chain Based System to Store and verify the Certificates by Creating an NFT. Connect your Metamask wallet to upload your Certificates and to ensure validation and Security. Enter your Certicate credentials to Verify your Certificate.

Figure 1: Synergy - Home Page

2. User Authentication and Authorization

- ✓ As illustrated in Figure 2, backend handles the user authentication and uses JWT for session handling and requesting processing.

- ✓ Admin/Auth User can upload the certificates, while Normal Users may view and confirm certificates only.

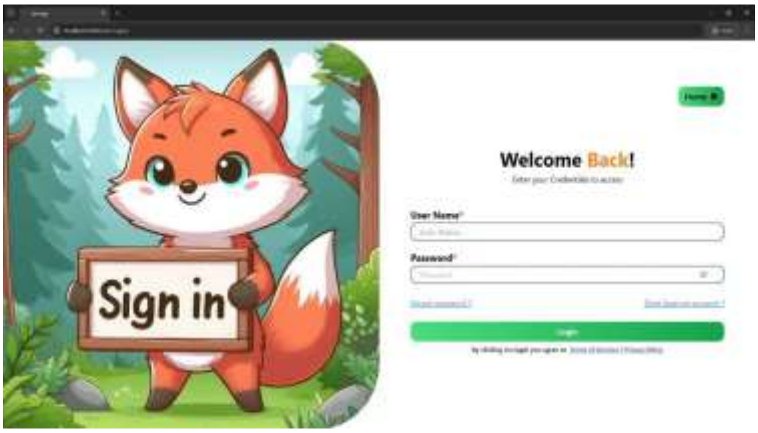


Figure 2: User Authentication Page

3. Backend (Server-side)

- ✓ Express.js is the backend framework for processing API requests. It directs incoming requests from the frontend, deals with user login, and directs interactions between the blockchain and databases.

- ✓ MongoDB acts as the NoSQL database where user profiles, metadata, and transaction data relating to the uploaded certificates are stored as depicted in Figure 3.

- ✓ Email.js is included to provide email alerts to the users whenever their certificates are uploaded or authenticated.

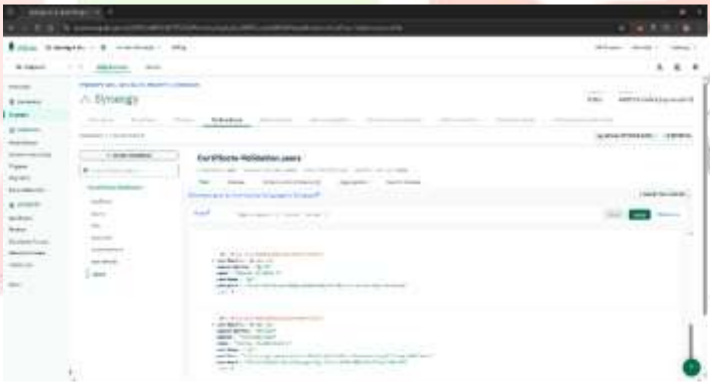


Figure 3: MongoDB

4. Blockchain Network

- ✓ Smart Contracts are authored in Solidity and deployed via Thirdweb. The smart contracts manage the certificate upload and verification process, with the data stored securely and immutably on the blockchain.

- ✓ MetaMask provides users with a means to interact with the blockchain network for executing transactions, including certificate uploads and verification. It is implemented as a digital wallet that securely connects users to the platform.

- ✓ As shown in Figure 4, Sepolia-ETH is utilized as a Testnet to execute blockchain transactions prior to going live on the Ethereum mainnet. It assists in testing smart contracts and transactions for accuracy and security.

Figure 4: Web3 – Base Sepolia Testnet

5. Data Storage and Cloud Integration

- ✓ Pinata is utilized for decentralized cloud storage to manage the storage of certificates and other related document data as illustrated in Figure 5. It enables users to obtain their certificates from an insecure, distributed network instead of centralized servers.

- ✓ AWS S3 is utilized for backup and storing large data files like images, PDFs, and other documents related to certificates. It provides scalability, reliability, and security.

Figure 5: Pinata – cloud storage

V. METHODOLOGY

The methodology for the Synergy Blockchain Project is structured around a systematic approach to build, deploy, and maintain a blockchain-based platform for certificate verification. The process follows a series of stages to ensure security, transparency, and user efficiency as shown in Figure 6.

1. Blockchain Design and Smart Contract Development In this step, blockchain design is planned and smart contracts are created that oversee the uploading of certificates, their verification, and safe storage.

    - ✓ Smart Contract Development: The logic of the uploading and verifying certificates is scripted through smart contracts in Solidity.

    - ✓ Smart Contract Deployment: Thirdweb is utilized to deploy the created smart contracts on the blockchain. This provides seamless management, updates, and scalability for the contract.

    - ✓ Testnet Deployment: Sepolia-ETH (testnet) is utilized to test all blockchain interactions to ensure validation of the smart contracts prior to mainnet deployment.

2. Backend Development Backend on the Synergy platform is written with Express.js for efficient management of data queries and API calls.

   ✓ RESTful API Development: The backend is built with Express.js to manage user authentication, certificates, and blockchain, cloud storage, and database interactions.

   ✓ Database Integration: MongoDB serves as the NoSQL database to securely store user information, certificate metadata, and transaction history.

   ✓ Email Integration: Email.js is integrated to send confirmation emails, upload certificate notifications, and other system alerts.

3. Frontend Development Frontend development is targeted towards giving an interactive interface for both Admin/Auth Users and Normal Users.

   ✓ UI/UX Design: The design is constructed utilizing Next.js along with Tailwind CSS for instant page loading and responsiveness. Libraries such as Ant-D, Shadcn, and DaisyUI have pre-existing UI components to deliver dynamic content like buttons, tables, modals, and forms.

   ✓ User Interaction: The frontend supports Admin users to upload certificates and Normal users to validate certificates related to their Gmail IDs. It interacts with the backend APIs to retrieve the necessary data and present it effectively.

   ✓ Blockchain Integration: MetaMask is integrated in the frontend to enable users to execute transactions and communicate with the blockchain. MetaMask is the digital wallet for executing secure transactions.

4. Blockchain Integration and Wallet Setup During this stage, the blockchain services integration and wallet management are established.

   ✓ MetaMask Integration: MetaMask must be installed and set up by users as their blockchain wallet to communicate with the Ethereum network.

   ✓ Blockchain Interaction: Admins are able to upload certificates through the platform, which communicate with the blockchain to securely store certificate information utilizing the launched smart contract.

5. Cloud Storage Integration To manage storage of documents, the project incorporates cloud services for storing certificates and other documents securely.

   ✓ Pinata Cloud Storage: Pinata is utilized to store certificate files in decentralized storage. Pinata saves files in a secure manner and makes certificates immutable and easily accessible when needed.

   ✓ ii) AWS S3: For bigger files and backups, AWS S3 is utilized to offer scalable, secure cloud storage, which ensures reliability and accessibility.

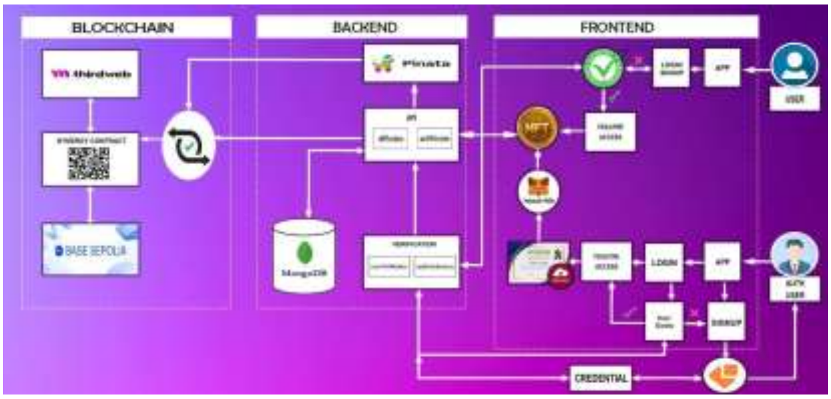


Figure 6: Architecture/Working

VI. IMPLEMENTATION

The system is developed using a combination of blockchain- based smart contracts, a robust backend, an intuitive frontend, and cloud-based storage solutions as shown in Figure 9.

1. Blockchain & Smart Contracts

- ✓ Solidity is used to develop smart contracts that handle certificate issuance, storage, and verification.
- ✓ Thirdweb is used for smart contract deployment on the Sepolia testnet before moving to the Ethereum mainnet.
- ✓ MetaMask is integrated for secure blockchain transactions.

2. Authentication & Security

- ✓ Google Sign-In (Passport.js) is integrated for secure user authentication.
- ✓ Role-based access control (RBAC) ensures that only authorized users can upload certificates.
- ✓ SSL encryption secures data transmission.

3. Payment & Live Support

- ✓ Stripe is used for subscription-based payments.
- ✓ Crisp Live Chatbot provides real-time user support.

4. Backend Development

- ✓ Express.js (Node.js) is used to build a RESTful API for handling certificate management and user authentication.
- ✓ MongoDB stores user details and certificate metadata.
- ✓ Pinata (IPFS) ensures decentralized storage of certificate files.
- ✓ The backend flow is as shown in Figure 7.

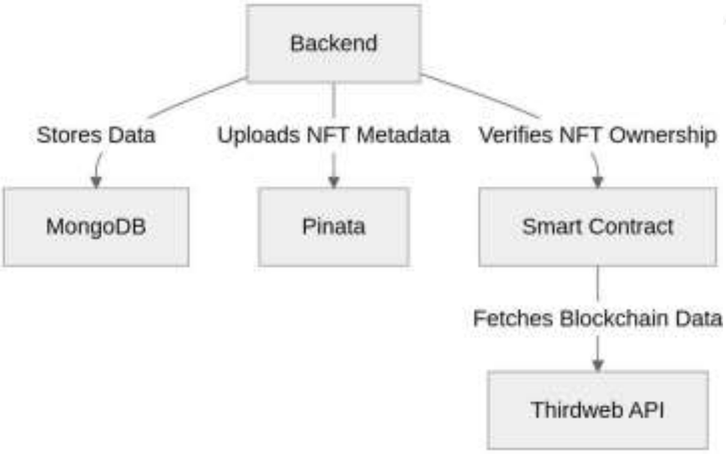
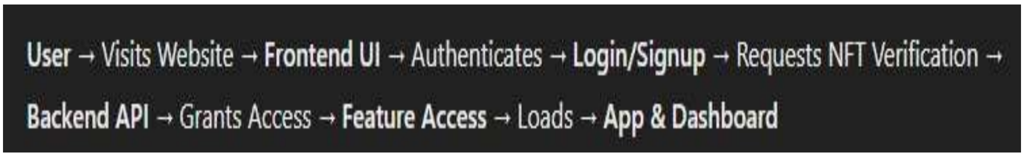


Figure 7: Backend flow

5. Frontend Development

- ✓ Next.js is used for a fast and interactive UI, with Tailwind CSS for styling.
- ✓ Ant-D, Shadcn, DaisyUI provide pre-built UI components.
- ✓ Web3.js/Ethers.js is used to enable interaction with blockchain smart contracts.



User → Visits Website → Frontend UI → Authenticates → Login/Signup → Requests NFT Verification → Backend API → Grants Access → Feature Access → Loads → App & Dashboard

Figure 8: Frontend flow

6. Deployment & Testing

- ✓ Backend and Frontend are made to run on the same port and are deployed as a single Project in Render.
- ✓ Smart contracts are deployed on ThridWeb (Base Sepolia testnet).
- ✓ Unit testing (Hardhat), API testing (Postman), and UI testing (Users feedback) ensure system reliability.

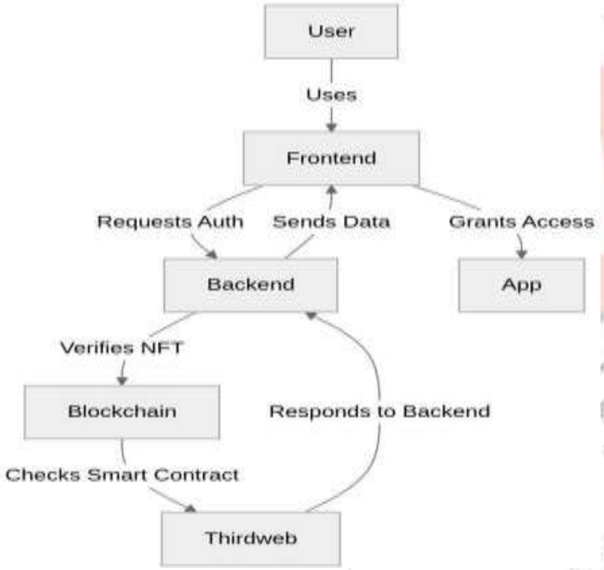
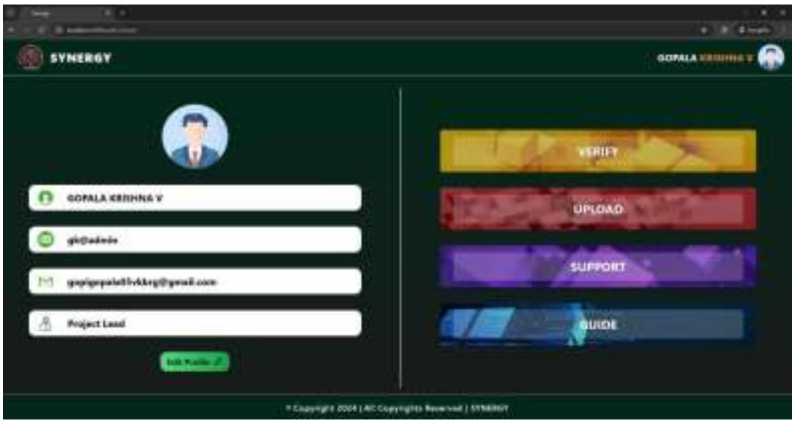


Figure 9: Complete Flow

VII. RESULT

On the frontend, Next.js is used for user interface as depicted in figure 10. The adoption of Tailwind CSS and UI libraries such as Ant-D, Shadcn, and DaisyUI enhances the interface's responsiveness and visual appeal. The system also integrates Stripe for secure payment processing and Crisp for 24/7 live support, improving user interaction and business scalability.



GOPALA KRISHNA V

gk@admin

gopigopala9vkkrg@gmail.com

Project Lead

Figure 10: User Page

The backend, developed with Express.js, efficiently handles API requests and ensures seamless communication between the frontend, blockchain, and database. MongoDB is used to store certificate metadata, while Pinata (IPFS) securely stores digital documents. Additionally, Email.js automates notifications, improving user communication and system efficiency as shown in Figure 11.

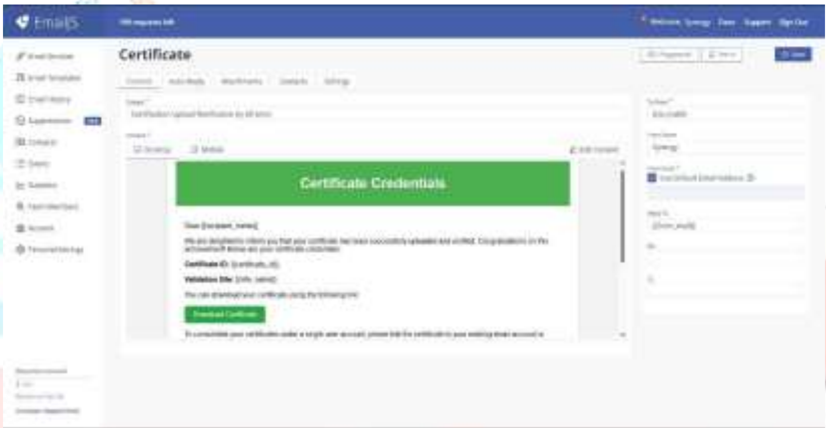
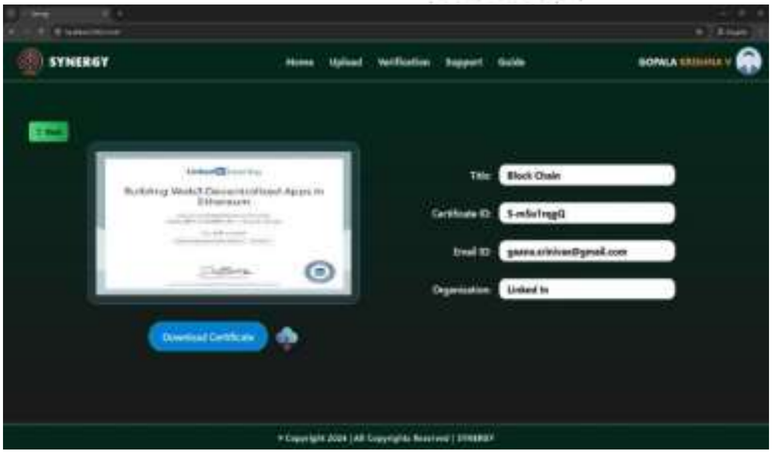


Figure 11: Email JS

The system's real-time certificate verification feature improves authenticity checks by reducing the need for manual validation. Interviewers and organizations can instantly verify a candidate's credentials through blockchain-stored records, ensuring trust and transparency in the verification process as shown in Figure 12.


SYNERGY
Home
Upload
Verification
Support
Guide
GOPALA KRISHNA V
Back
Building Web3 Decentralized Apps in Ethereum
Download Certificate
© Copyright 2024 | All Copyrights Reserved | SYNERGY

Title: Block Chain

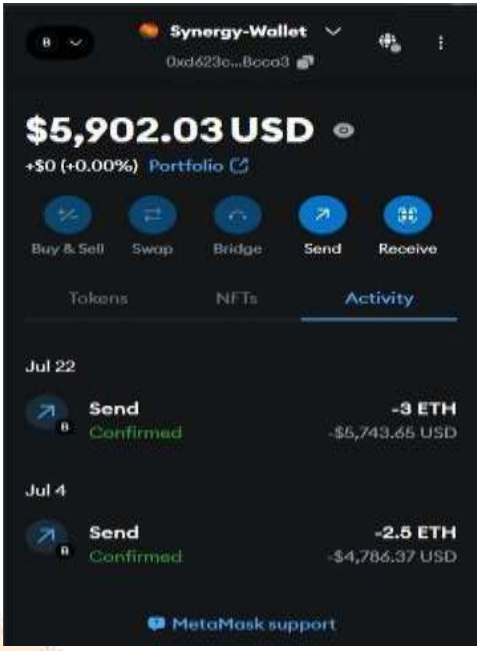
Certificate ID: S-m5o1rqgQ

Email ID: gaana.srinivas@gmail.com

Organization: Linked In

Figure 12: Verified Certificate

Implementing Solidity for smart contracts and deploying them via Thirdweb, the system ensures that certificates remain immutable and protected from forgery. The integration of Metamask as a digital wallet as shown in figure 13 and the use of Sepolia-ETH as a testnet currency facilitate smooth and secure transactions.



$5,902.03 USD

+$0 (+0.00%) Portfolio

Jul 22

Send Confirmed -3 ETH -$5,743.65 USD

Jul 4

Send Confirmed -2.5 ETH -$4,786.37 USD

Figure 13: Metamask Wallet

The backend, developed with Express.js, efficiently handles API requests and ensures seamless communication between the frontend, blockchain, and database. MongoDB is used to store certificate metadata as shown in Figure 14, while Pinata (IPFS) securely stores digital documents.

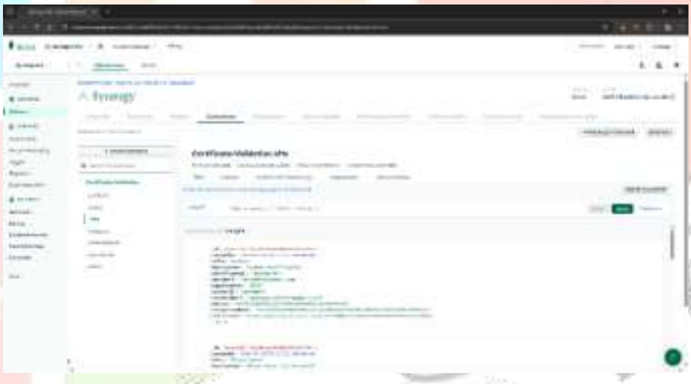


Figure 14: Mongo DB

VIII. CONCLUSION

The Synergy Blockchain Certificate Validation System provides a secure, decentralized, and tamper-proof solution for credential verification. By leveraging blockchain technology, certificates are stored immutably, ensuring authenticity and preventing fraud. The integration of smart contracts automates the validation process, eliminating manual verification and reducing administrative burdens. With blockchain's transparency and security, the system ensures that credentials remain verifiable and accessible at all times.

Overall, this project represents a transformative shift in digital credential verification by enhancing trust, efficiency, and security. By eliminating fraud risks and streamlining verification, it reduces paperwork and administrative efforts while ensuring seamless access to authenticated certificates. The decentralized approach makes it a reliable, scalable, and future-proof solution for educational institutions, businesses, and individuals, offering a more efficient and trustworthy alternative to traditional certificate validation methods.

IX. FUTURE SCOPE

The future scope of the synergy project can involve the integration of advanced technologies like AI and blockchain to enhance user experience. AI-powered tools could streamline certificate validation, detect fraud, and offer personalized recommendations. Additionally, interoperability with other blockchain platforms and external verification systems could broaden the system's utility, ensuring seamless integration across various industries. The platform can also embrace newer blockchain protocols to improve scalability and speed, keeping up with technological advancements.

Further user-centric features could include customizable portfolios where users not only showcase certificates but also incorporate other verifiable achievements like degrees, licenses, and project portfolios. Enhanced analytics could provide insights into users' certificates, improving the decision-making process. The system could also introduce more advanced authentication measures, ensuring high security while expanding its reach to various sectors like education, healthcare, and professional certification bodies.

References

[1] “Blockchain Technology for Secure Document Management and Verification.”
star.informatik.rwth-aachen.de/Publications/CEUR-WS/Vol-2280/paper-10.pdf

[2] “Enhancing Digital Credential Authentication Using Blockchain.”
https://ijsra.net/sites/default/files/IJSRA-2022-0225.pdf

[3] "The Impact of Decentralized Identity Management on User Privacy and Security.”
https://esource.dbs.ie/server/api/core/bitstreams/062eec4b-d16e-4562-8076-643ddc3439f8/content

[4] “Improving Resume Verification Through Blockchain- Based Credentialing Systems."
https://ijettjournal.org/Volume-72/Issue-8/IJETT-V72I8P113.pdf

[5] “User Experience and Accessibility in Digital Certificate Management Systems.”
https://is.muni.cz/th/396249/fi_m/DP-lenkahorakova.pdf

[6] “Email-Based Notification Systems for Digital Credential Distribution.”