International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 12– No.45, August 2024 – www.ijais.org

Utilizing Blockchain Technology for University Certificate Verification System

Olaiya Samuel Oluwaseyi
Department of Information System and Security, School of Computing, Federal University of Technology Akure, PMB 704, Akure, Ondo State, Nigeria

R.O. Akinyede
Department of Information System and Security, School of Computing, University of Technology Akure, PMB 704, Akure, Ondo State Nigeria

ABSTRACT
In the contemporary digital age, the authentication and verification of academic certificates have become increasingly vital yet challenging due to issues such as fraud, forgery, and the inefficiencies of traditional paper-based systems. This paper explored the implementation of blockchain technology as a robust solution for university certificate verification systems. Blockchain's decentralized, immutable ledger offers unparalleled security, transparency, and trust, making it an ideal framework for certifying academic credentials. By leveraging blockchain, universities can issue tamper-proof digital certificates that are easily verifiable by employers and other stakeholders, eliminating the need for intermediaries. This system enhances the reliability of academic records, reduces administrative burdens, and accelerates the verification process. Moreover, the paper discusses the technical architecture of a blockchain-based certificate system, including smart contracts, cryptographic techniques, and distributed consensus mechanisms. The paper analyze case studies of existing implementations to highlight the practical benefits and challenges encountered. The findings suggest that blockchain technology not only fortifies the integrity of academic certifications but also paves the way for a more efficient, transparent, and globally accessible verification infrastructure. This transformative approach has the potential to set new standards in academic administration and significantly curb credential fraud on a global scale.

General Terms
Degree certificates, Certificate falsification, Certificate Authentication.

Keywords
Blockchain, Ethereum, Smart Contract, Swarm, Ganache, Docker bee factory.

1. INTRODUCTION
Higher institution of learning issue certificates to graduates to demonstrate their qualifications upon successfully completing their chosen courses. These degree certificates and transcripts are crucial records required for job applications and further education. With the increasing number of transcripts and certificates issued annually by educational institutions, the problem of fake transcripts and certificates remains significant [1]. Graduation certificates are often Paper-based documents, as electronic documents cannot fully replace physical certificates.

With millions of graduates seeking employment every year, manually validating their certificates is time-consuming and exhausting. Monitoring and validating such a large number of record is extremely challenging, creating an environment where false or cloned certificates can be generated through tampering. This issue has led to a rise in fraudulent organizations engaging in the unethical practice of falsifying academic degrees. Technological advancements have made it increasingly difficult to distinguish between authentic and fraudulent certificates [4]. Consequently, the validation and verification of documents have become more important. It is crucial to confirm the authenticity of graduates' certificates and ensure that the rightful owner possesses them. Traditional paper certificates require significant effort and resources and are susceptible to fraud due to errors and forgeries. Additionally, paper-based mark sheets are not easily accessible, lack flexibility, are time-consuming, and are not environmentally friendly. The availability of inexpensive modern technologies has exacerbated the issue of certificate forgery, posing risks to both certificate bearers and the issuing universities [2].

This research propose a digitalized verification method for degree certificates using blockchain technology. Blockchain's immutability ensures that degree certificates are free from fabrication and falsification [4]. Blockchain is a digital ledger technology that securely stores and verifies transactions across numerous computers or nodes, being decentralized and distributed. Although initially designed as the foundational technology for the cryptocurrency Bitcoin, its applications extend far beyond virtual currencies. It is considered a component of the fourth industrial revolution, enabling transactions to be validated and secured, and data to be updated in a transparent, synchronized, and decentralized manner with a majority consensus system [5].

Blockchain is a decentralized, immutable database consisting of a sequence of "blocks" containing data such as transaction dates, times, amounts, and participants [6]. A cryptographic identification mechanism uniquely identifies participants when one user initiates a transaction with another via a peer-to-peer network. The transaction is then transmitted to the blockchain network storage pool, awaiting verification. A new block is created after reaching a certain number of authorized nodes, achieving consensus. Following agreement, a new block is created, and each node updates its corresponding blockchain ledger copy, a process known as mining. Proof of Work (PoW) and Proof of Stake (PoS) are two common consensus procedures [7].

Blockchain is immutable because it is a distributed ledger maintained by thousands of nodes, making tampering successful only if 51% of the ledgers are modified via the network [8]. Furthermore, blockchain is transparent as data recording is visible to each node on the network, even when data is updated. Blockchain is also traceable since all transactions are sequentially ordered, with each block associated with its adjacent blocks using a hash function. Thus, each transaction can be tracked by checking block information [7].

The benefits of blockchain technology in education range from information handling to data verification without sacrificing accuracy. Blockchain-based solutions can streamline and simplify administrative tasks, such as validating issued credentials like

degrees, transcripts, and students' qualifications, successes, and professional abilities [8]. Furthermore, blockchain solutions allow students to retain ownership and control over their obtained credentials, eliminating the need for intermediaries to verify them [9].

2. RELATED WORKS

Research by [12] addresses the issue of fraudulent educational certificates through the development of a digital certificate system using blockchain technology. As the number of colleges, students, and graduates increases, there is a greater need for a straightforward and cost-effective method of verifying degree certificates. Students seek low-cost, easily verifiable documentation, while employers require quick and reliable degree verification. This study proposes a blockchain-based digital certificate system for securely storing and verifying educational certificates in a decentralized manner. The researcher designed a smart contract that allows only the owner to add institutions to the system. Each generated certificate is stored in the Interplanetary File System (IPFS) with a unique hash created using the SHA-256 technique, and both the hash and certificate data are stored on the blockchain. This system reduces administrative costs, prevents document counterfeiting, and provides accurate and reliable digital certificate information.

In [11], the application of blockchain technology in higher education is explored. The researchers provide a critical analysis of the opportunities and constraints associated with blockchain technology in this sector, particularly its impact on educational development. The study includes real-world applications, with the Massachusetts Institute of Technology (MIT) serving as an example. Using the multivocal literature review (MLR) technique, which includes grey literature from sources such as newspapers, blogs, websites, and government documents, supplemented by peer-reviewed academic literature, the researchers identify the benefits and limitations of blockchain in education. However, the study primarily focuses on the advantages and disadvantages of blockchain technology rather than thoroughly analyzing the technical aspects of its implementation. It also lacks a comprehensive examination of the potential impact of blockchain technology on the entire educational system. Research by [13] emphasizes the problem of counterfeit certificates and the need for a reliable system to verify academic credentials. The proposed system utilizes the Ethereum blockchain network to store the hash of certificates, while the IPFS (Interplanetary File System) stores the actual certificates, ensuring data immutability and security. This decentralized system for verifying academic credentials offers a secure and unchangeable method for storing and verifying certificates. The study suggests that this method can be extended to other industries requiring time stamping of digital documents.
The study by [14] proposes a blockchain-based system capable of producing, authenticating, and validating academic certificates. This system addresses concerns about certificate authenticity, provides quick responses, and ensures reliable and secure storage. The system involves two actors: the university (admin) and other users (students/employers). The university can create new certificates, make necessary modifications, and authenticate certificates, while general users can only verify the authenticity or view the certificates without making changes. The proposed system ensures certificate authenticity and secures the decentralized system. However, one limitation is that it requires significant computational resources, which can increase implementation costs.

Research by [10] focuses on certificate verification using blockchain technology. The researcher suggests a blockchain-based solution to the problem of certificate forgery. The proposed method involves digitizing original paper certificates, creating a hash code value using a chaotic technique, and adding this to the blockchain. Leveraging the blockchain's immutability, the approach aims to enhance information privacy and prevent certification fraud in the future.

There are numerous structural problems with the current methods of academic certificate administration. These include the ease with which tangible certifications can be faked and the often manual, cumbersome processes required to validate academic achievements. Such issues undermine the credibility of academic credentials and create obstacles for all stakeholders involved. Blockchain technology offers a paradigm shift in data handling by promising enhanced security, efficiency, and trust. Given these persistent issues, a blockchain-enabled solution is necessary. While blockchain is best known for its role in cryptocurrencies, it has the potential to revolutionize various sectors, including business, education, and healthcare. This research explores the application of blockchain technology in education, specifically focusing on certificate management.

3. METHODOLOGY

The Ethereum blockchain serves as the backbone to this system, providing a decentralized framework essential for establishing a trustless environment where transactions are both transparent and secure. Unlike traditional centralized databases, Ethereum's distributed ledger technology offers a robust defense against data manipulation and fraud. Ethereum is particularly well-suited for our application due to its support for smart contracts. These programmable contracts automate complex processes, such as the issuance and verification of certificates, and enforce the rules of engagement within the blockchain network. Additionally, Ethereum's consensus mechanism initially Proof of Work (PoW) and transitioning to Proof of Stake (PoS) ensures network security and transaction validity. These mechanisms are crucial for maintaining the integrity of the academic records stored on the blockchain.

In the current methodology, the university follows the standard process to generate a digital certificate, which can be an image or PDF, depending on the school's practices. In the proposed system, the university continues to generate digital certificates as usual; this system does not create the certificates itself. Instead, it provides a mechanism for managing and verifying these certificates on the blockchain.
In the system architecture depicted in Fig 1, an administrator (Admin), appointed by the university, upload digital certificate to the block-chain and these administrators are only needed at the period when the university need to upload certificate to the block-chain. Once the certificate is uploaded, the blockchain ensures the certificates' authenticity and immutability, allowing for secure and efficient verification without further intervention from the administrators.

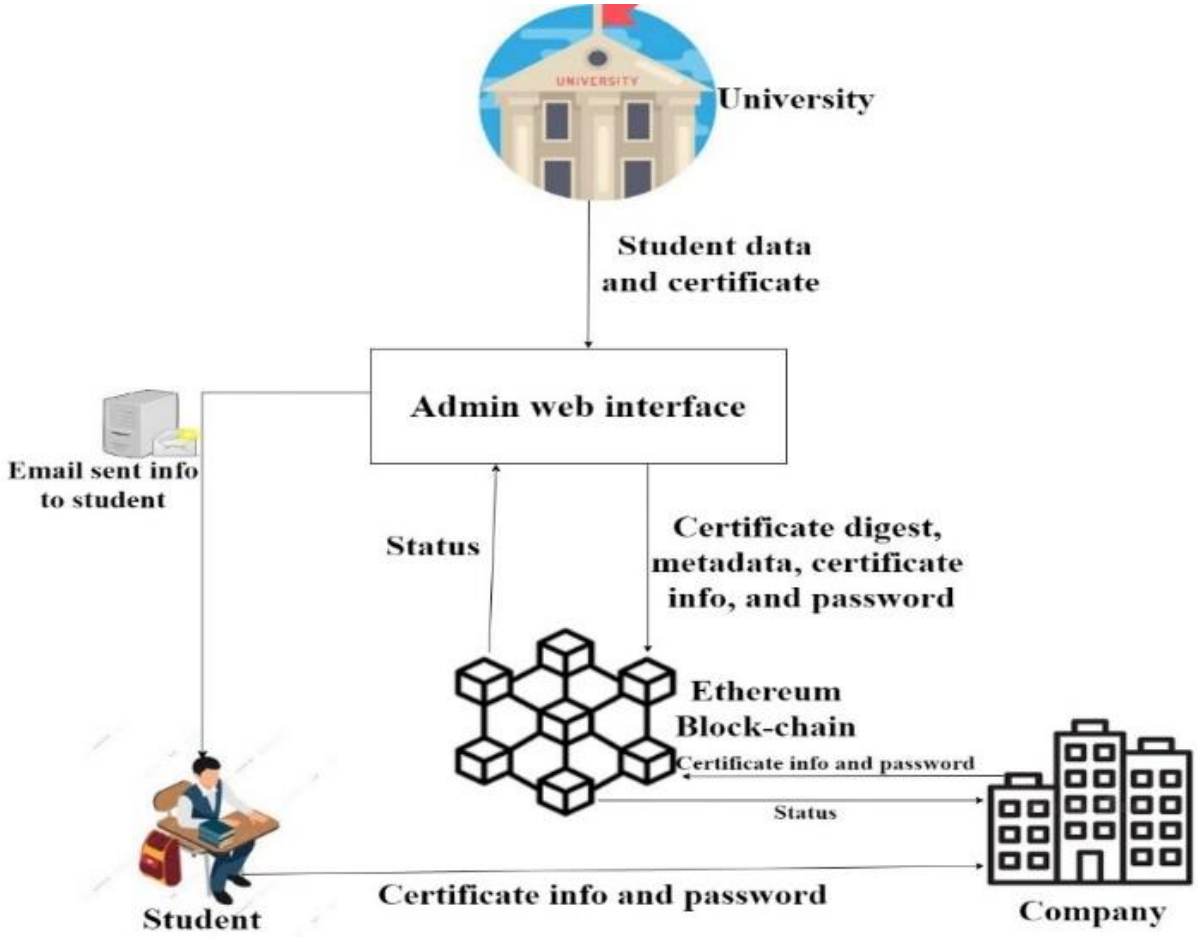

Fig 1: System architecture of the proposed system

Fig 2 provides a detailed architectural breakdown of our blockchain-based academic certificate verification system. Our system's blueprint, or architecture, shows how different components and technologies interact together to create a seamless and effective platform. The interaction between the various parts of the suggested system is depicted in the diagram below.

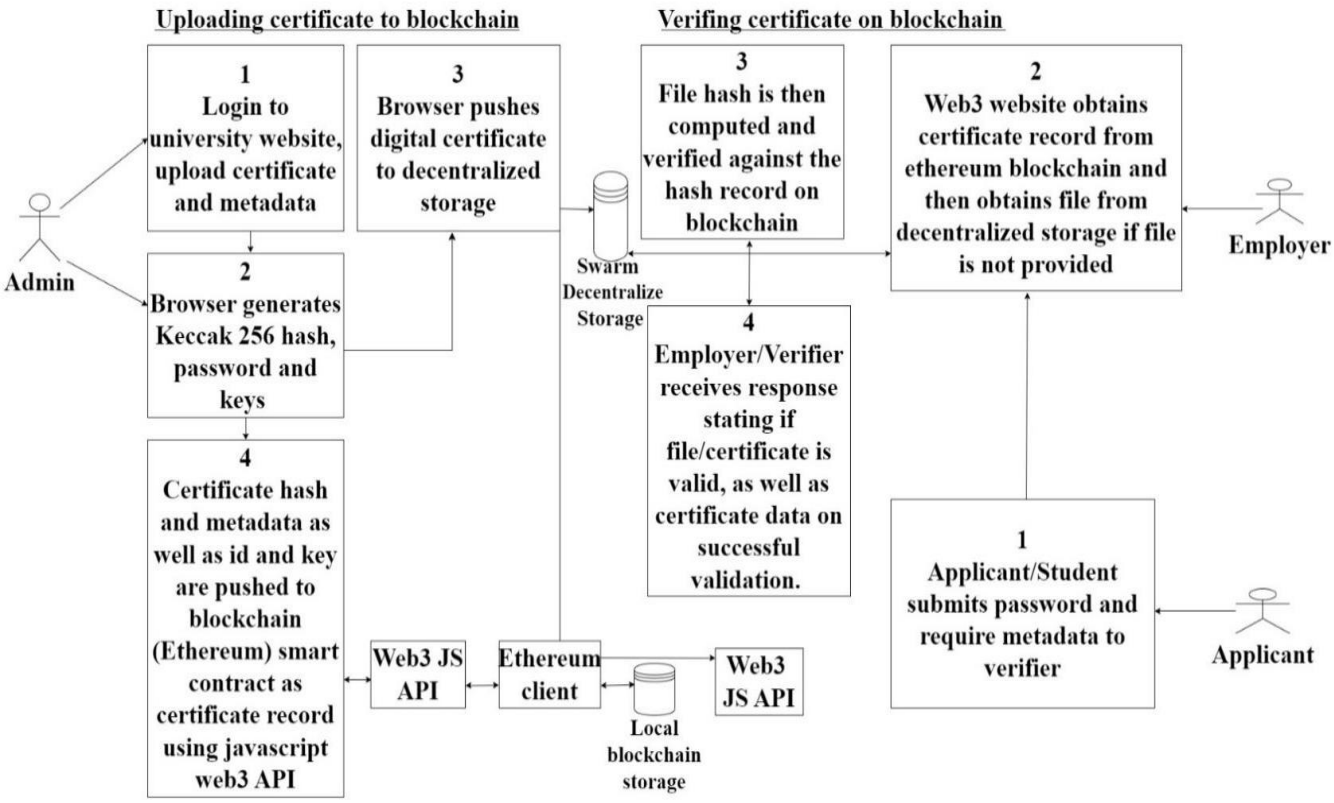

Fig 2: The components of the proposed system, particularly the upload and verification process.

The Ethereum client represents the blockchain in which the smart contract and certificate data is deployed to, below is a typical illustration of the Ethereum client:

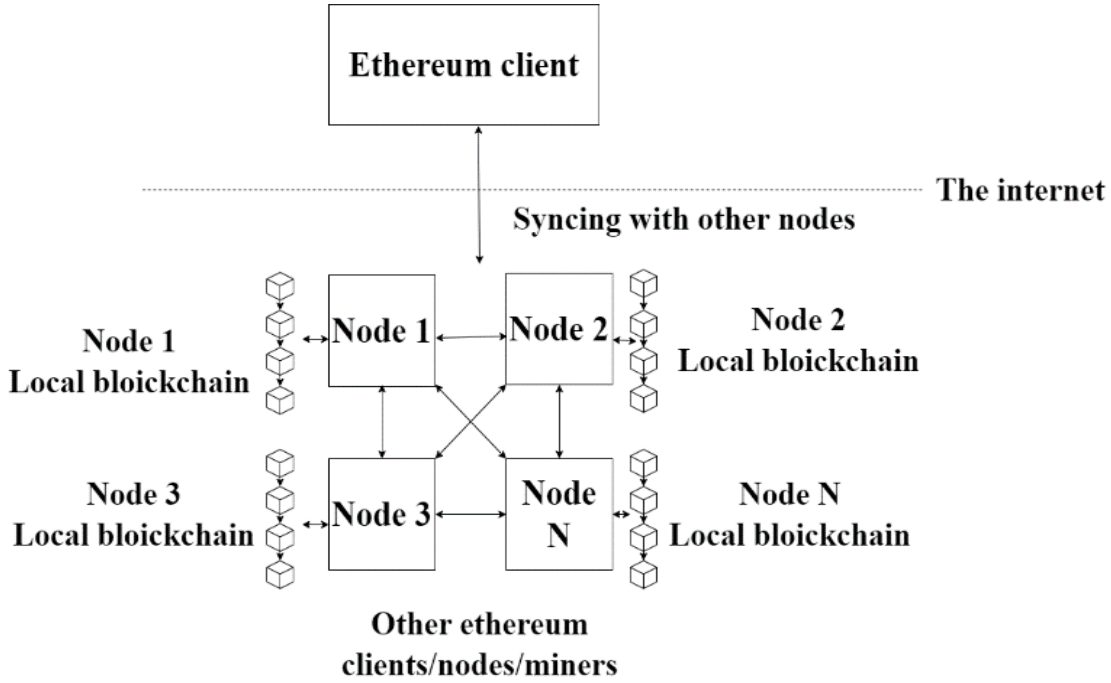

Fig 3: A typical representation of an Ethereum client showing the Interaction between nodes and their localized blockchain storage.

3.1 Detailed Description of the Upload System (Interface)

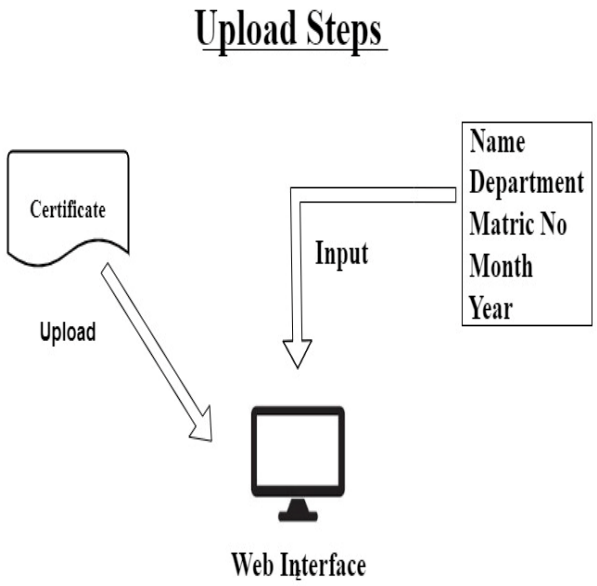

Fig 4: Certificate Upload & Metadata input

In the certificate upload process, the upload interface is used by the administrator (assigned by the institution) to upload a certificate and associated metadata to the Ethereum blockchain through communication with the smart contract that has been established. From Fig 4 above, the following is a list of the steps and internal mechanisms involved in the certificate upload process:

1. Certificate Upload by the Administrator: The university administrator (Admin) plays a crucial role in the proposed blockchain-based certificate verification system, as they upload the digital certificate to the browser (Dapp). This stage aims to smoothly combine the Ethereum blockchain's technological benefits with the real-world requirements of educational establishments.

a) **Admin Interface and Login**: The Admin accesses the system through a secure web interface, developed using React, and enhanced with HTML, CSS, and JavaScript for a robust front-end experience. This interface serves as the entry point, where the Admin logs into the university's dedicated portal for certificate uploads (Upload Interface).

b) **Uploading Certificate Files and Entering Metadata:** The Administrator uploads the original certificate files after logging in. These files, which are usually in JPEG or PDF format, show the students' real certificate. The administrator simultaneously enters significant metadata related to every certificate. This metadata includes the student's name, matriculation number, department and the date of issuance.

c) **Integration with Ethereum Blockchain:** The front-end interface, using Web3 API, facilitates direct communication with the Ethereum blockchain. This connection is essential for the integrity and decentralization of the system. The Admin utilizes a MetaMask plugin, installed on the browser, to interact with the Ethereum network. The MetaMask wallet holds Ethereum crypto currency (private keys), which is essential for covering gas fees associated with blockchain transactions.

d) **Smart Contract Deployment and Interaction:** A smart contract, residing on the Ethereum Virtual Machine (EVM), deployed via truffle, manages the certificate data. The addition of new certificate data to the blockchain involves interaction with this smart contract. This process incurs gas fees, underscoring the need for the MetaMask wallet.

e) **Communication with JSON RPC via Web3.js**: The browser communicates with the Ethereum blockchain using JSON RPC (JavaScript Object Notation Remote Procedure Call) through the Web3.js library. This library converts user requests into JSON RPC requests, which are then transmitted to the local Ethereum node.

f) **Transaction Processing and Blockchain Entry:** The local Ethereum node, upon receiving the request from the MetaMask wallet, forwards it to the mining nodes for processing. At the end of this process, the data is safely kept on the blockchain, guaranteeing the academic credentials' transparency and immutability.

2. Hash Generation and Secure 5-word Mnemonic Creation: Following the successful upload of certificate files to the web interface explain below, the system advances to an important security phase, focusing on hash generation and secure password (mnemonic) creation depicted in Fig 5 below.

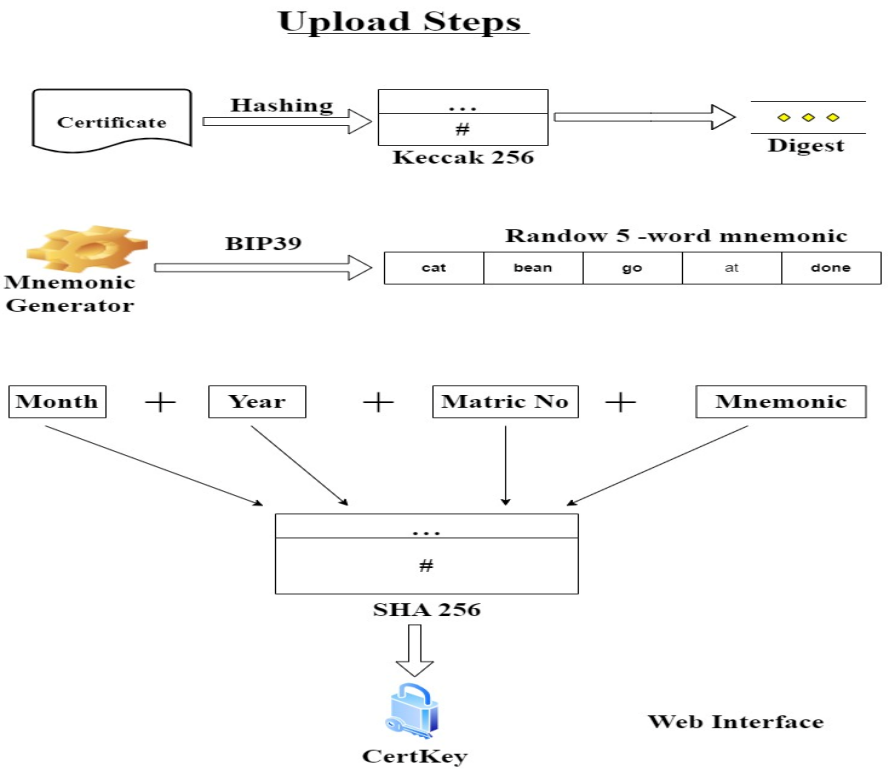

Fig 5: Digest, Mnemonic & *Certkey* Generation

a) Generation of Keccak-256 Hash: The core of this step lies in generating a unique identifier for each certificate file. This is achieved through the Keccak-256 hashing algorithm, a variant of SHA-3. The Web3.js API plays a pivotal role here, transforming the digital certificate file, be it a PDF or an image, into a distinct Keccak-256 hash. This hash serves as a unique digital fingerprint, ensuring that each file is represented by an immutable and singular hash on the blockchain.

b) Secure Password Creation: Simultaneously, the system generates a 5-word mnemonic as password. This 5-word mnemonic follows the BIP39 standard. This password creation process is designed to be collision-resistant, ensuring that each password is unique and secure. The generation mechanism is crucial for maintaining the integrity of the verification process, as it adds an additional layer of security, as verification requires this mnemonic which acts as a kind of authorization.

c) Next a 256 bit certificate key (CertKey) is generated by concatenating the month, year, matric number and mnemonic and then computing the SHA3-256 digest of the result. This string serves as the key to the certificate data (value) in the blockchain. The certificate data is stored in a mapping data structure (a HASHMAP data type).

3. Decentralized Storage with Swarm: The third step as depicted in Fig 6 below, involves interfacing with Swarm, Ethereum's decentralized storage system, to securely store the digital certificate files.

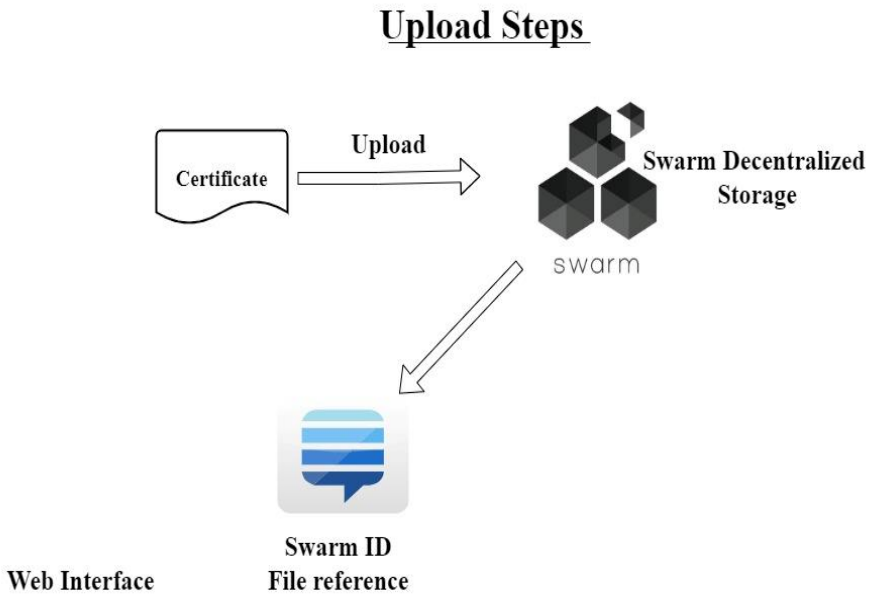

Fig 6: Digital Certificate upload to swarm

a) **Uploading to Swarm:** Using the Web3.js package to provide the required functionality, the browser starts the process of uploading the digital certificate file to Swarm. This procedure makes sure that the actual certificate file is kept in a decentralized fashion, taking advantage of Swarm's distributed network's security and redundancy advantages.

b) **Retrieval ID Generation:** Swarm creates a special ID (Swarm ID) for the file after a successful upload. By serving as a point of reference, this ID makes it possible to efficiently retrieve the certificate from the decentralized storage. It's necessary to make sure the certificate file is always readable and verified in the system.

c) **Sending Students a Digital File and Swarm ID:** Along with the mnemonic, the digital certificate is sent to the student via mail, while the Swarm ID is added to the metadata of the certificate that is uploaded to the Ethereum blockchain. This ID is a critical component for the verification process, allowing students and other verifying entities to access the certificate file from Swarm via the verification interface, after the verification process is completed.

4. Blockchain Transaction for Certificate Validation: The final step in the certificate upload process involves the actual blockchain transaction depicted in Fig 7, which includes storing the certificate hash and associated metadata on the Ethereum blockchain. The following steps explain the block-chain transaction of the certificate upload process:

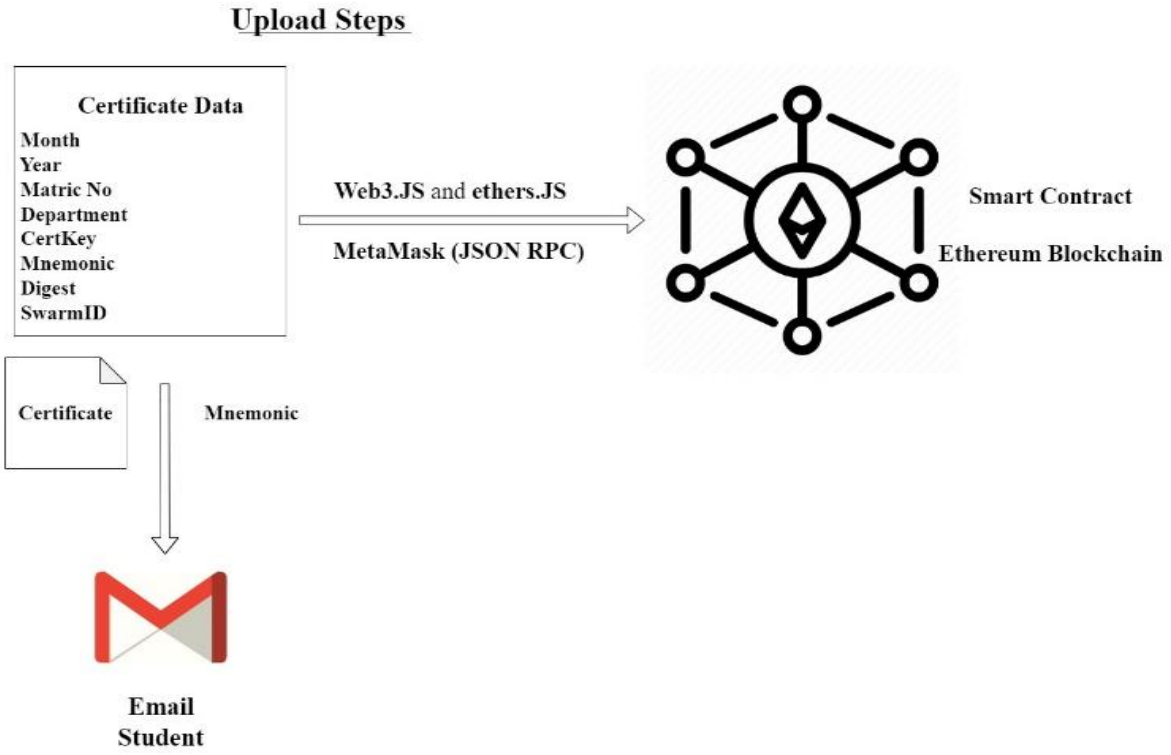

Fig 7: Certificate Metadata Upload to Blockchain

a) **Data Preparation for Blockchain**: The system prepares the following data for the blockchain transaction: the Keccak-256 hash of the certificate, the 5-word BIP39 generated mnemonics (certificate password), the Swarm ID, the ***Certificate Key*** and the certificate's metadata (names, matriculation number, department, month, and year of issuance). The certificate Key is generated from the certificate metadata (matriculation number, month, year and mnemonics) and is used as the key for the certificates metadata in the blockchain as the data is stored in a ***mapping*** data structure (HashMap).

b) **Web3 API and Ethereum Client Interaction**: The Web3 API, integrate to this process, is responsible for creating the JSON RPC requests that communicate with the Ethereum client. This interaction is critical for ensuring that the certificate data is correctly formatted and transmitted to the blockchain.

c) **MetaMask Wallet Transaction**: The Admin, using the MetaMask wallet installed in the browser, initiates the blockchain transaction. This transaction involves sending the prepared data to the Ethereum network, which requires Ethereum gas fees to be paid. The MetaMask wallet facilitates this payment, enabling the transaction to be processed by the Ethereum miners. The address that deployed the certificate is the only address that can upload certificate or an addressed that has been assigned by this address.

d) **Storing Data on the Blockchain**: The certificate data, including the hash, password, metadata, and Swarm ID, is securely stored on the Ethereum blockchain. This storage is immutable, meaning that once the data is recorded on the blockchain, it cannot be altered or deleted, thus ensuring the integrity and verifiability of the certificate.

e) **Transaction Confirmation and System Integrity**: Once the transaction is confirmed on the blockchain, the system's integrity is upheld. The uploaded certificate data is now securely embedded in the blockchain, available for future verification by any authorized party, including employers, other educational institutions, or the students themselves.

This final step completes the certificate upload process, effectively leveraging the blockchain's decentralized and immutable nature to ensure the security and verifiability of academic certificates. It highlights the system's sophisticated use of Ethereum's blockchain technology, smart contract functionality, and decentralized storage solutions to address the challenges in traditional certificate verification processes.

3.2 Certificate Verification Process.

In the Certificate verification process the *Verification Interface* is used. This verification interface can be accessed by a student, company, an institution, or anyone with access to the required certificate metadata and the 5-word mnemonic (certificate password). The verification involves several steps and internal workings as listed in Fig 8 below:

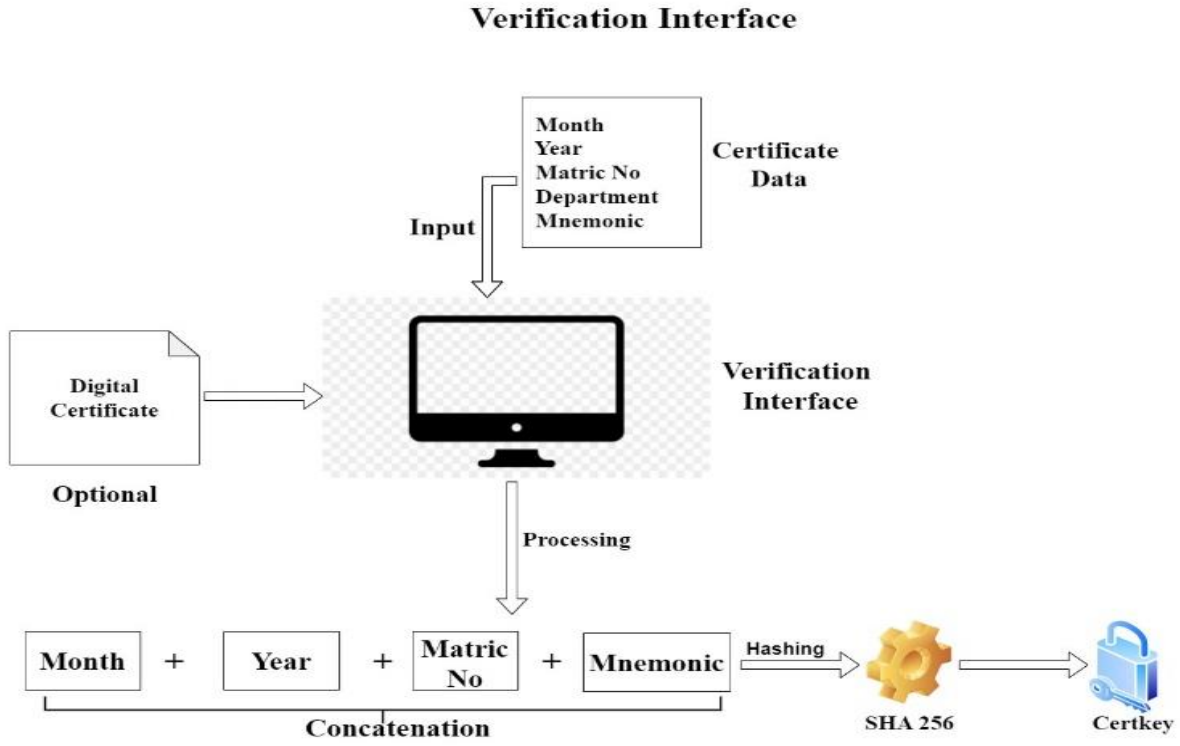

Fig 8: Certificate data Input and CertKey Generation

a) **Applicant's Submission**: The verification process begins with the applicant or student submitting the original digital certificate if is it available, along with the mnemonic and required metadata to the verifier (employer or institution). The required data includes the *Date* (month & year), *matriculation number*, *department,* and the *5-word mnemonic* (certificate password provided by the student). Next the verification interface regenerates the certificate key by concatenating the required metadata and running the result through a hash function – *SHA3-256* – to obtain

the 256 bit certificate key (**CertKey**) for this certificate. The CertKey will be used to query the Ethereum blockchain for the full certificate metadata. The certificate metadata is stored in a key/value data structure (mapping).

b) **Retrieving Certificate Record**: With the help of the ***Web3.js*** and ***Ethers.js*** modules using a JSON RPC request call from Fig 9 below, the verification interface attempts to obtain the full certificate metadata from the Ethereum
block-chain using the certificate key (***CertKey***) generated in the previous step. This transaction does **NOT** required money (ETH).

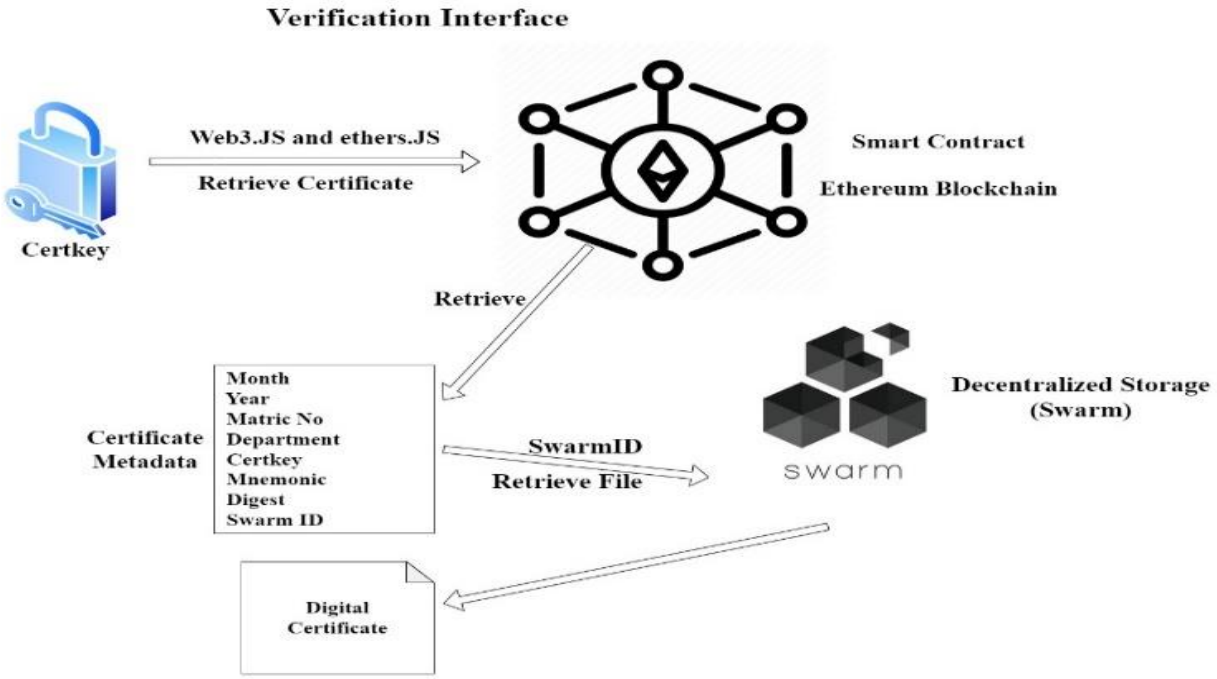

Fig 9: Metadata and digital certificate retrieval

From Fig 9 above, if the retrieval is no successful, it will return the corresponding certificate metadata associated with the CertKey provided, otherwise it will return an error if the certificate does not exist or the CertKey is not associated with any valid certificate. For a valid response, the ***Swarm ID*** is extracted from the metadata returned and is used to query the swarm decentralized storage for the original file (Digital certificate). This step will not be performed if the verifier uploads a file to the verification interface.

c) **Hash Verification**: From fig 10 below, the system computes the hash (Keccak-256 digest) of the submitted certificate file compares it against the hash recorded on the blockchain. This step is crucial for verifying the authenticity of the certificate.

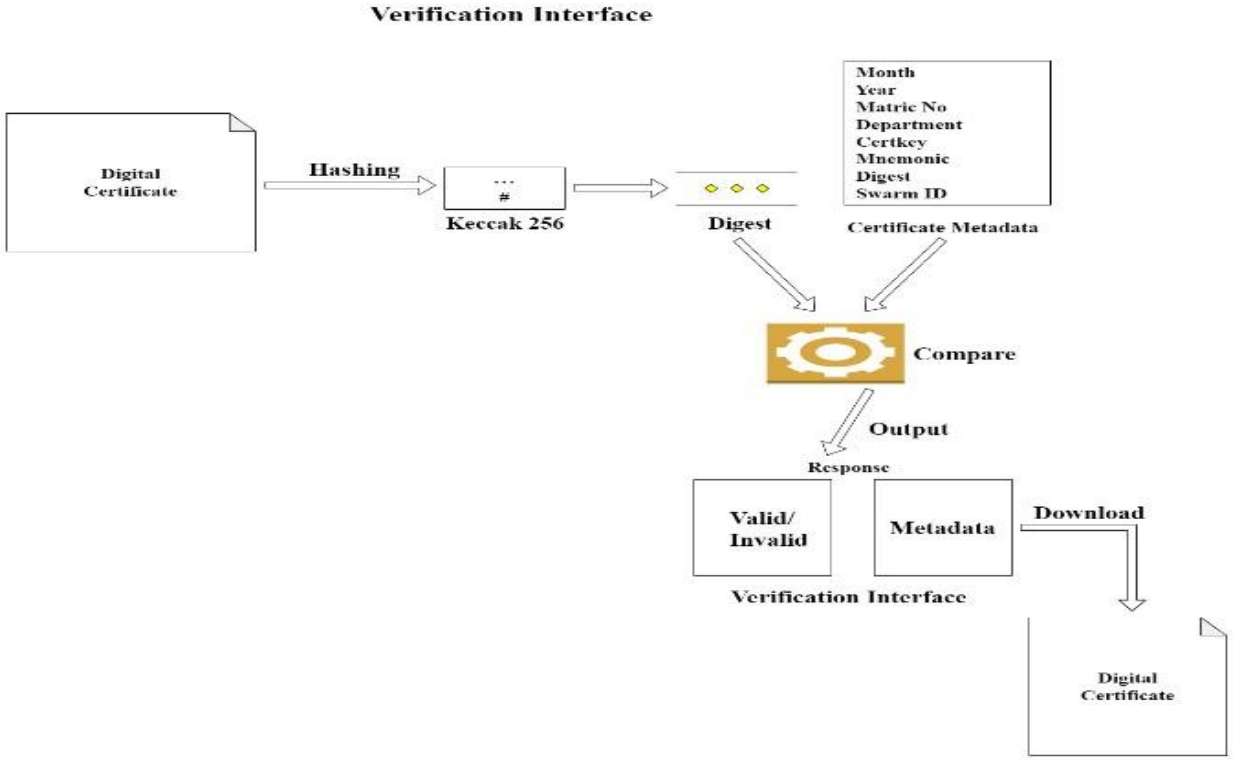

Fig 10: Certificate Verification and Results

d) **Validation Response**: Upon successful hash comparison, the employer or verifier receives a response indicating the validity of the certificate. If the hashes match, it confirms the certificate's authenticity. Additionally, the Ethereum smart contract provides the associated metadata, offering further validation of the certificate's legitimacy.

3.3 Mathematical Algorithm

3.3.1 The algorithm for certificate upload stages

1. Admin uploads certificate:

let F be the digital certificate file, and $K(F)$ is the $keccak256$ digest of the (F) then the certificate hash is generated as follows:

$K(F) = keccak256(F)$ (1)

let $M, Y, B\ P, G$ be the month on the digital certificate (eg "05), the year on the digital certificate (eg "2023"), the matriculation number on the certificate ($e.g$ "$CSC/09/8213$"), a randomly generated five words mnemonic, and G is the concatenation of M, Y, B, P respectively.

$G = M + Y + B + P$ (2)

$K(G) = keccak256(G)$ (3), where $K(G)$ is the $keccak256$ digest of G

2. Store digital certificate on swarm and certificate metadata on Ethereum virtual machine:

$S = Swarm(F)$ (4) where $Swarm(F)$ represents the storage of the digital file of the certificate on swarm, returning a Swarm ID as S

$V = (K(F), G, P, S, M, Y, B, E)$ (5), where V is the tuple containing all the metadata and identifiers.

Store V on ethereum:
$Ethereum(V)$ (6), $Ethereum\ (V)$ represents the storage of V on the Ethereum block-chain in a mapping with G as the key.

The model for certificate verification stages:

3. Certificate verification:

let $M!, Y!, B!, P!$ equals to the month on the digital certificate provided by the verifier, the year on the digital certificate provided by the verifier, the matriculation number on the certificate provided by the verifier, the password generated by the browser provided by the verifier respectively.

$G! = M! + Y! + B! + P!$ (7), where $G!$ is the concatenation of $M!, Y!, B!, P!$

Retrieve $V!$ from ethereum using ! :
$V! = Ethereum^{-1}[G!]$ (8), where $V!$ is the value obtained from blockchain

Retrieve $(K(F), G, P, S, M, Y, B, E)$ from $V!$

Retrieve F from swarm using S:
$F^1 = Swarm^{-1}[S]$ (9)

Compute $keccak256$ of the file according to the following:

$K(F!) = keccak256\ (F)$ (10), where $K(F!)$ is the keccak of the file generated by the verifier

Check digests equality of the digital certificate:
$K(F!) == K(F)$ (11), where $K(F)$ is the $keccak$ generated by the web interface of the admin.

The model will be implemented using:

(i) Truffle Suite: Used for developing, testing, and developing Ethereum smart contracts,
(ii) Ganache: Create a personal Ethereum blockchain for testing smart contract
(iii) Matamask: A browser extension wallet for interacting with the ethereum blockchain
(iv) React and Redux: For building a dynamic and responsive user interface, and
(v) Web3.JS and Ethers.JS: JavaScript libraries for blockchain interaction.

3.4 Verifying a Certificate

The user Interface for certificate verification is also a simple form, in which the verifier enters the public certificate metadata (Date and Matriculation number) and the certificate mnemonic or password. This password should only be known by the certificate owner (the student) as it was sent to their email at the time of upload. The verifier can also upload the digital certificate if they have it. The digital certificate is optional as the verification interface will obtain it from swarm. When the user clicks on "VERIFY CERTIFICATE", the verification interface first reconstructs the certificate key from the metadata provided and then used it to obtain the full certificate metadata from the blockchain. It extracts the swarm ID from the metadata and uses it to fetch the digital certificate from the Swarm network, after which the actual verification process is performed, after which a dialog appears showing if the certificate is valid or not. Certificate verification does not require gas fee, but the user also has to connect their MetaMask wallet to the interface with a valid account for the blockchain.

4. DISCUSSION & EVALUATION

The efficacy of a system can be measured by user feedback on its functionality, ease of use, and the time and effort required to understand it. Thirty students interacted with our system, and we evaluated their level of satisfaction. The feedback indicated that the system was highly useful and user-friendly, with many students expressing a desire to use it regularly.
This blockchain-based certificate verification system has demonstrated high effectiveness and efficiency in automating the upload and verification of academic certificates. By leveraging the Ethereum blockchain and decentralized storage with Swarm, the system ensures that all transactions are immutable and transparent, providing a robust solution to the issues inherent in traditional manual verification processes. Compared to the manual process, where students apply for transcripts that are then sent via email to the verifying organization, the blockchain system significantly reduces the time required for verification. This automation eliminates human errors and fraud, and mitigates risks associated with email-based communication, such as data tampering and loss of confidentiality. By streamlining the verification process, the system not only enhances security but also improves the overall efficiency and reliability of academic certificate management.
We conducted a survey to gather user feedback on various aspects of the blockchain-based system, including overall satisfaction, efficiency, speed, security enhancement, user-friendliness, and transparency. The results indicate high user satisfaction with the system's accuracy, reliability, and transparency. Users appreciated the immutable and secure nature of the blockchain, which significantly enhanced the trustworthiness of the certificate verification process.

However, the survey also highlighted areas for potential improvement. Some users suggested enhancements to the user interface design to make it more intuitive and visually appealing. Additionally, there were calls for better technical support to assist users in navigating and utilizing the system effectively. Addressing these areas can further enhance the user experience and ensure the widespread adoption of the blockchain-based certificate verification system.

The horizontal bar plot in Fig 11 below provides a clear visual representation of the average ratings for different aspects of the blockchain-based certificate verification system. Each bar corresponds to a survey question, and its length represents the average rating given by respondents.
The results indicate high satisfaction levels in categories such as overall performance, efficiency, and transparency, with average ratings close to 5. These high ratings suggest that users find the system reliable and effective.

However, areas like technical difficulties and user-friendliness show more variability in ratings, indicating potential areas for improvement. Specifically, addressing technical issues and enhancing the user interface could further improve overall user satisfaction. By focusing on these areas, the system can become even more user-friendly and accessible, ensuring a smoother and more efficient experience for all users.

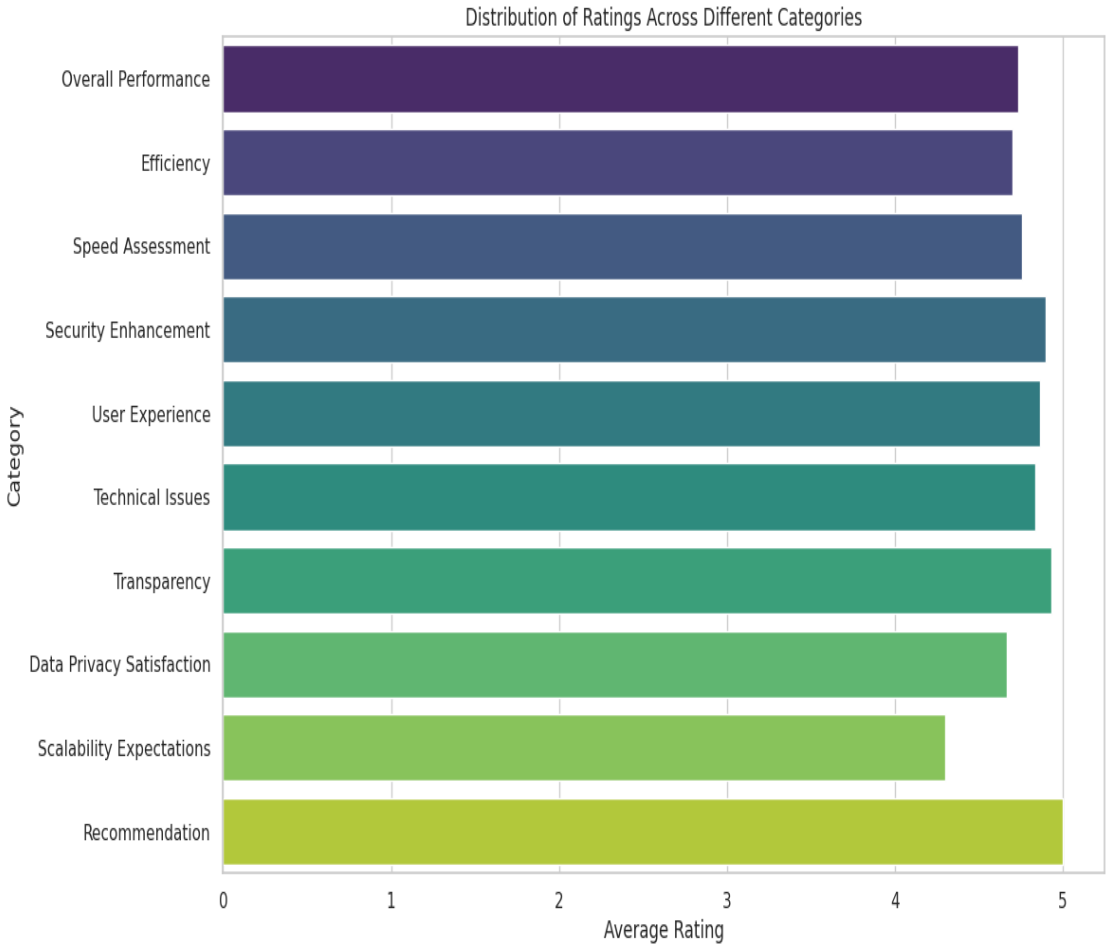

Fig 11: Horizontal Bar Plot analysis of question

It also highlights areas where responses were more varied, suggesting where further investigation and improvements may be needed. By focusing on these areas, such as technical difficulties and user-friendliness, the system can continue to evolve and meet user needs more effectively.

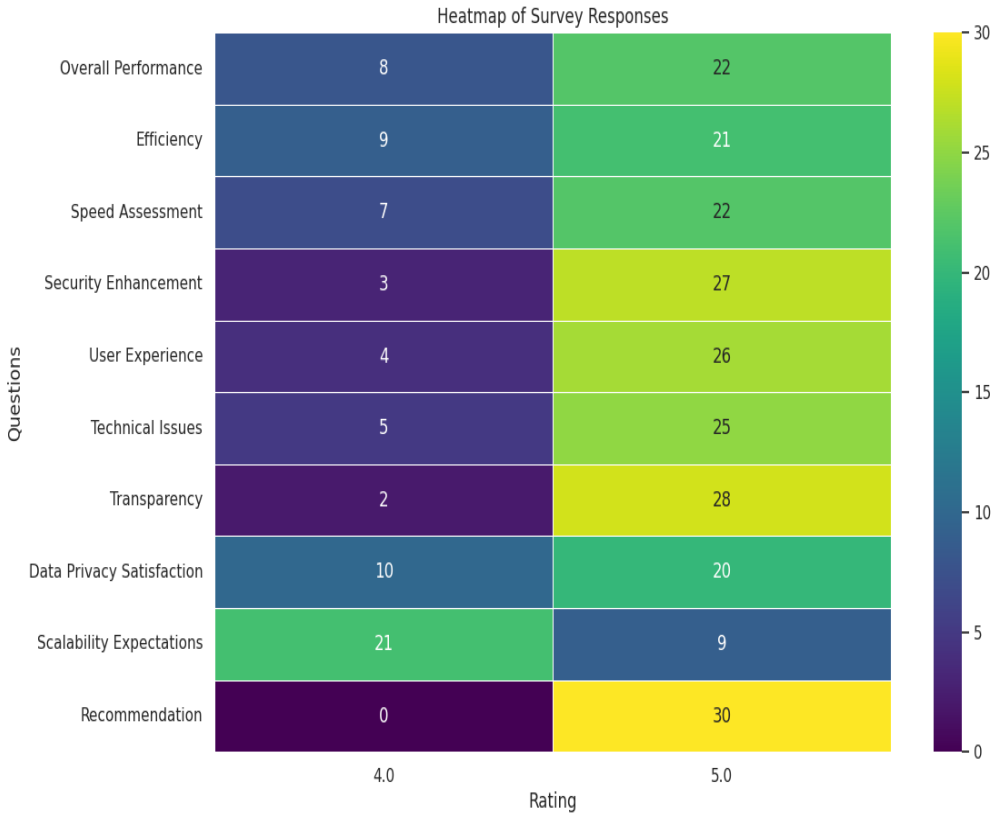

Fig 12: Heat Map result on response

Analysis: Fig 12 above shows the heat map result on response of the students. The heat map offers a detailed view of the distribution of ratings across different survey questions. Each cell shows the count of responses for a specific rating (from 1 to 5) for each question, with color intensity representing the frequency. Darker colors indicate higher frequencies, making it easy to identify dominant ratings. The heatmap reveals that most questions received high frequencies of ratings 4 and 5, indicating positive user feedback.

This visualization helps identify trends, such as consistently high satisfaction with the system's accuracy, reliability, and transparency. It also highlights areas where responses were more varied, suggesting where further investigation and improvements may be needed. By focusing on these areas, such as technical difficulties and user-friendliness, the system can continue to evolve and meet user needs more effectively.

5. CONCLUSION

The integration of blockchain technology into university certificate verification systems represents a significant advancement in the management and authentication of academic credentials. By providing a decentralized, immutable, and transparent framework for issuing and verifying digital certificates, blockchain addresses critical issues such as credential fraud, inefficiencies, and administrative burdens that plague traditional systems. This research has demonstrated the effectiveness of a blockchain-based system in ensuring the security, reliability, and efficiency of certificate verification processes.

While the current implementation has proven successful, there are several avenues for future exploration and improvement. One potential area for future research is the expansion of this system to support a broader range of academic credentials, including transcripts and diplomas across multiple educational institutions. Additionally, integrating this blockchain-based system with existing educational management systems could further streamline administrative processes and enhance user experience.

Future work could also explore the use of advanced consensus mechanisms and scaling solutions to improve the system's performance and reduce transaction costs, making it more accessible for widespread adoption. Furthermore, the integration of artificial intelligence and machine learning could provide enhanced capabilities, such as predictive analytics for detecting fraudulent activities or automating the verification process.

Lastly, addressing regulatory and legal challenges will be crucial for the global adoption of blockchain-based certificate verification systems. Establishing standardized protocols and ensuring compliance with international data protection laws will be essential. for building trust and ensuring the widespread acceptance of this innovative approach.

In conclusion, the application of blockchain technology in academic credential verification has the potential to revolutionize educational administration, providing a secure, efficient, and globally accessible solution that sets new standards for trust and transparency in the digital age.

6. REFERENCES

[1] Warasart, M., & Kuacharoen, P.: Based document authentication using digital signature and QR code. In *4TH International Conference on Computer Engineering and Technology (ICCET 2012)*.

[2] Sheng, C. A. O., Zheng, C., & Xuandong, S. *2007* Anti-counterfeit Authentication System of Printed Information Based on A Logic Signing Technique. In *International*

Conference on Intelligent Systems and Knowledge Engineering. pp. 1254-1259

[3] Gopal, N., & Prakash, V. V. 2018 Survey on blockchain based digital certificate system. *International Research Journal of Engineering and Technology (IRJET)*, *5*(11)

[4] Otuya, J. A. 2019 *A blockchain approach for detecting counterfeit academic certificates in Kenya* (Doctoral dissertation, Strathmore University).

[5] Bozic, N., Pujolle, G., & Secci, S. 2016 A tutorial on blockchain and applications to secure network control-planes. *3rd Smart Cloud Networks & Systems (SCNS)*, 1-8

[6] Ma, Y., & Fang, Y. 2020 Current status, issues, and challenges of blockchain applications in education. *International Journalof Emerging Technologies in Learning (IJET)*, *15*(12),
20-31,

[7] Chen, G., Xu, B., Lu, M., & Chen, N. S. 2018 Exploring blockchain technology and its potential applications for education. *Smart Learning Environments*, *5*(1), 1-10

[8] Kulkarni, M., & Patil, K. 2020 Block chain technology adoption using toe framework. *Int. J. Sci. Technol. Res*, *9*(2), 1109-1117

[9] Kamišalić, A., Turkanović, M., Mrdović, S., & Heričko, M. 2019 A preliminary review of blockchain-based solutions in higher education. In *Learning Technology for Education Challenges: 8th International Workshop, LTEC 2019, Zamora, Spain, July 15–18, Proceedings 8* (pp. 114-124). Springer International Publishing

[10] Ahmed, B., Raza, M. O., Farooqui, M. A., Baig, M. A., & Aziz, M. A. 2022 Certificates Verification on the Block Chain. *Journal of Optoelectronics Laser*, *41*(7), 186-190

[11] Fedorova, E. P., & Skobleva, E. I. 2020 Application of blockchain technology in higher education. *European Journal of Contemporary Education*, *9*(3), 552-571

[12] Badhe, V., Nhavale, P., Todkar, S., Shinde, P., & Kolhar, K. 2020 Digital Certificate System for Verification of Educational Certificates using Blockchain. *International Journal of Scientific Research in Science and Technology*, *7*(5), 45-50

[13] Charitha, T. S., & Baba, K. A. 2022 A System for Academic Certificates Verification Using Blockchain. *Int J Res Appl Sci Eng Technol*, *10*(6), 3392-3397

[14] Rahman, M. M., Tonmoy, M. T. K., Shihab, S. R., & Farhana, R. 2023 Blockchain-based certificate authentication system with enabling correction. *arXiv preprint arXiv:2302.03877*.

7. APPENDIX

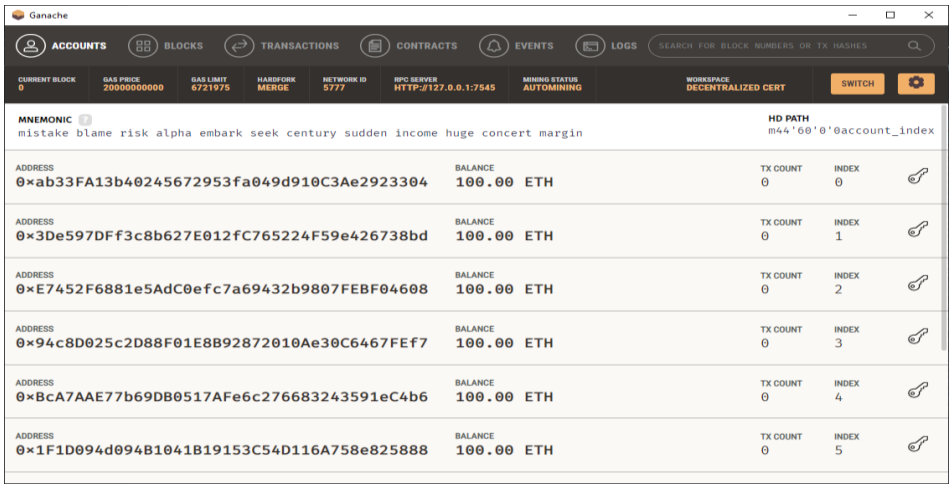

Fig 13: Local Ethereum Blockchain Implementation with Ganache

The fig 13 shows the local Ganache blockchain after it has been set up and configured. Ganache provides 10 accounts with a default value of 100ETH per account, which is more than sufficient for testing.

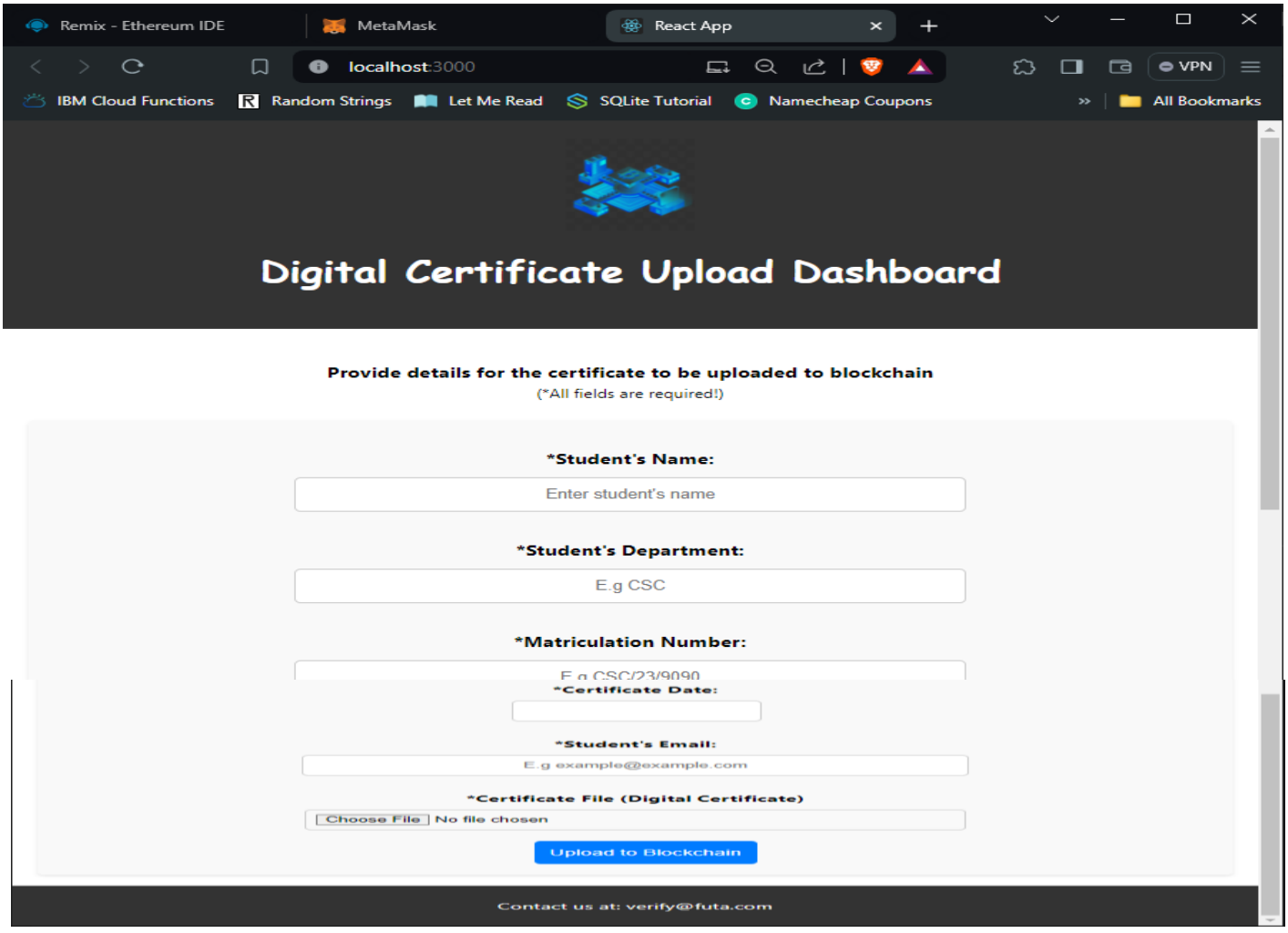

Fig 14: The diagram shows the upload interface form.

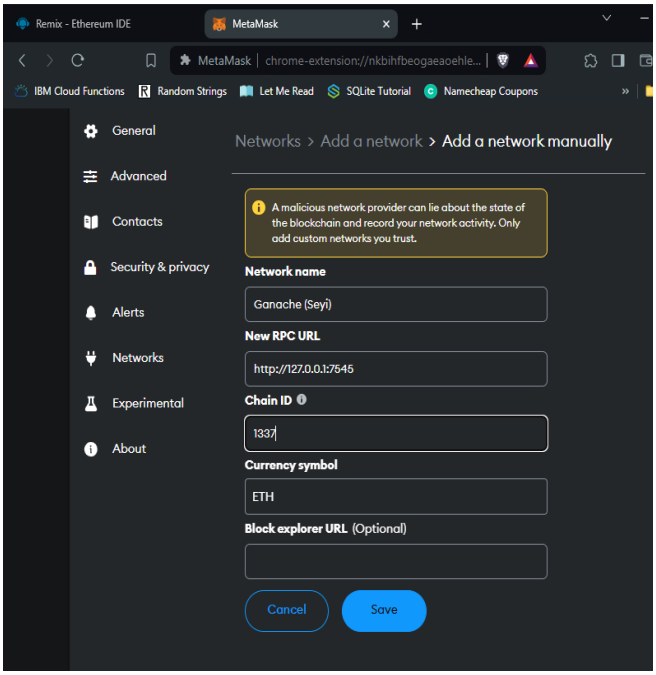

Fig 15: Adding the Local Ganache Blockchain to MetaMask. The main component is the RPC URL and the Chain ID

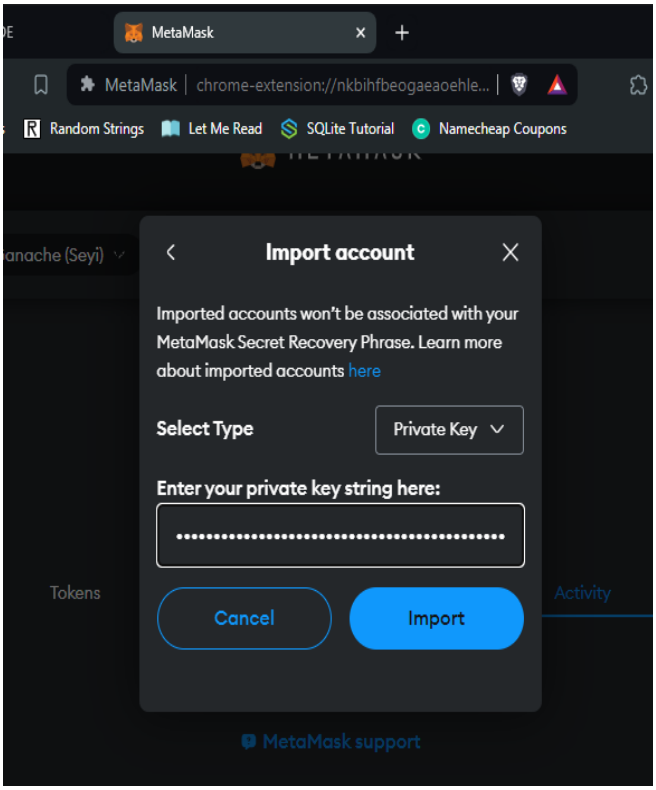

Fig 16: Importing a Ganache account to MetaMask using its private key.

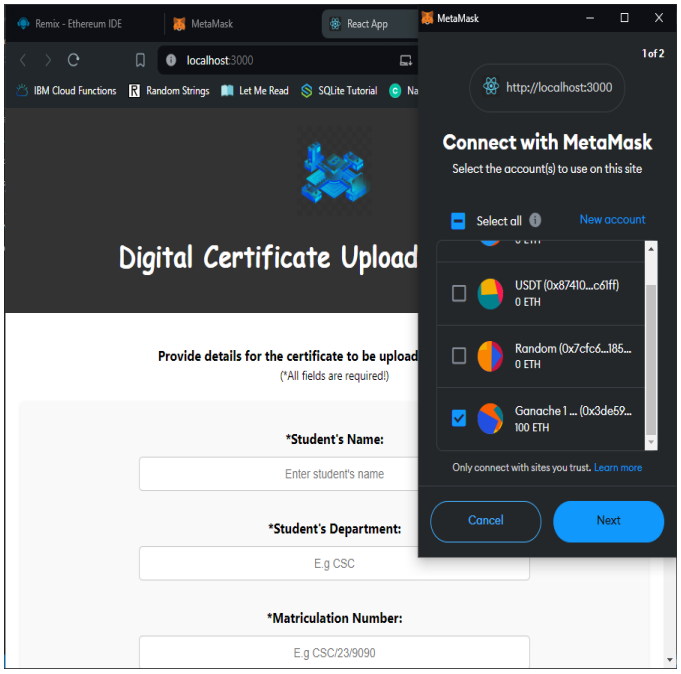

Fig 17: Admin connects their wallet to the upload interface

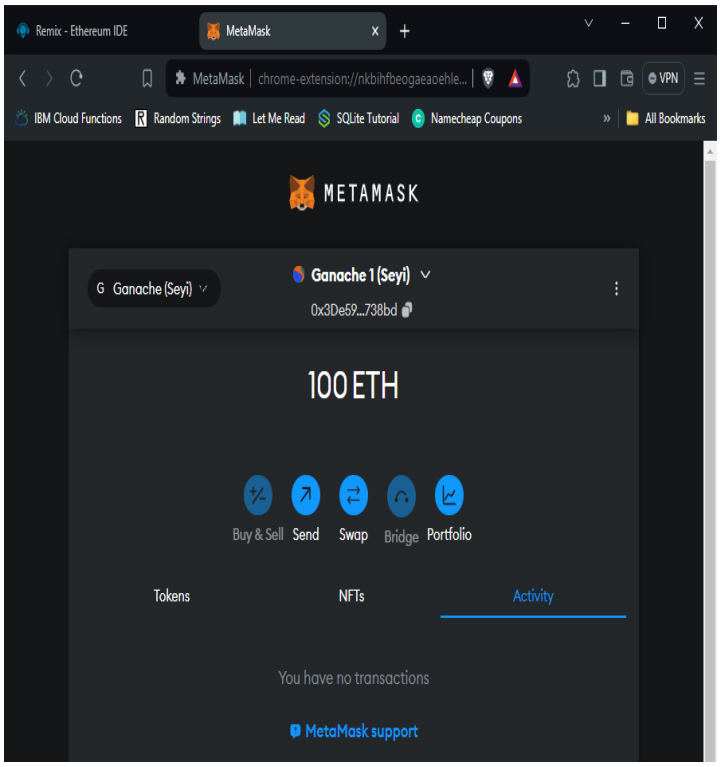

Fig 18: Imported Ganache account showing the initial 100ETH

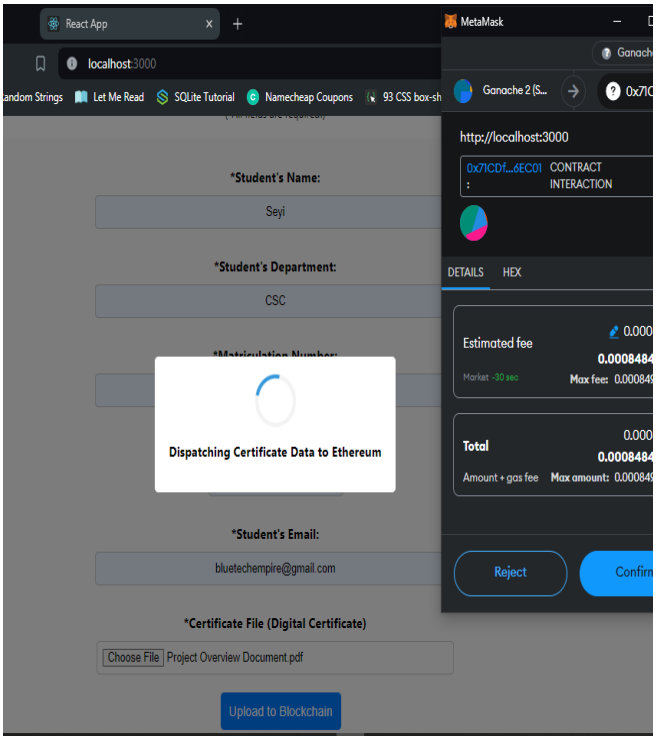

Fig 19: Image showing the upload process, after the certificate metadata and digital file is uploaded to the browser and metadata is being uploaded to Ethereum blockchain. The admin must confirm the transaction, as an amount of ETH will be spent as gas fee. This confirmation is provided by MetaMask which acts as the browsers gateway to the Ethereum blockchain

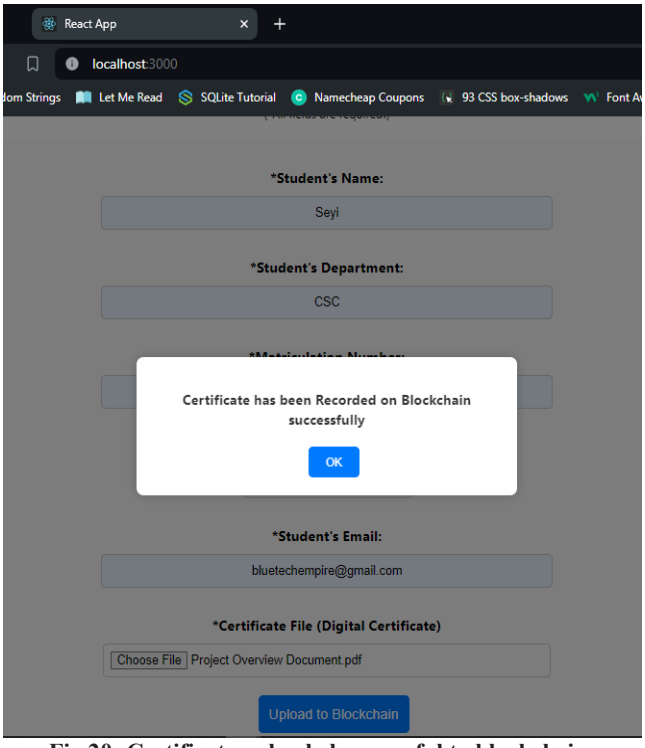

Fig 20: Certificate uploaded successful to blockchain

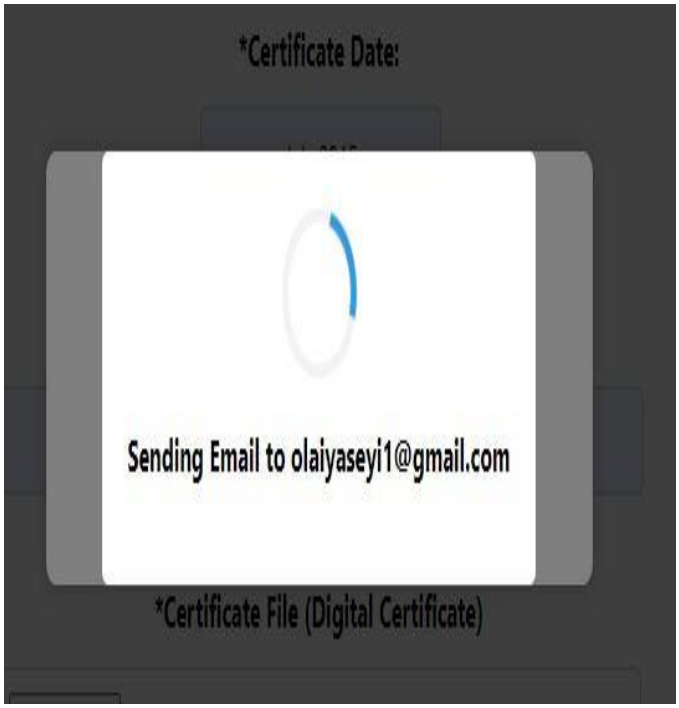

Fig 21: Certificate email to student

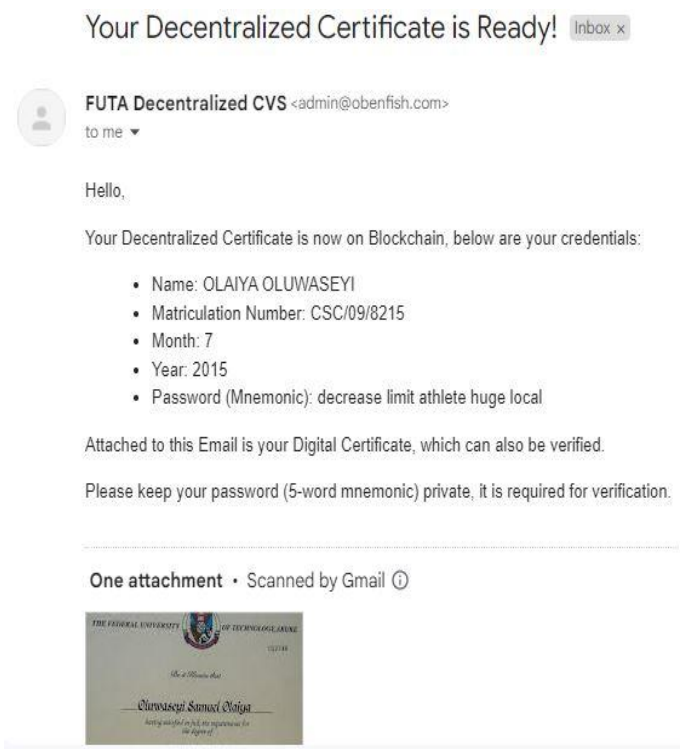

Fig 22: Certificate metadata & digital Certificate received by the student