DEVELOPMENT OF A DECENTRALISED MODEL FOR ELECTRONIC EXAMINATION PASS USING BLOCKCHAIN TECHNOLOGY

[1]Olaniyan O.M. and[2*]Adekoya T. F.

[1,2]Department of Computer Engineering, Federal University, Oye Ekiti
Corresponding Author, email: olatubosunadekoya@gmail.com

ABSTRACT

Conventional examination pass systems face persistent challenges of security breaches and administrative inefficiencies due to the centralised nature of these systems. There is a need to address the problem of centralisation to enhance the security of these systems and fortify the integrity of the examination process by mitigating the risks of data manipulation and unauthorized access. This study introduces a decentralised framework, powered by Hyperledger Fabric private blockchain, to revolutionize examination pass management. A unique channel is established for the administrator to maintain a ledger of registered students and their examination pass information, enabling seamless sharing with peer nodes. Subsequently, distinct artifacts, including a Membership Service Provider (MSP), a Certificate Authority (CA), and an ordered node, are established to facilitate administrative rights, assign digital identities, and order transactions, respectively using cryptographic protocols. Security analysis show that the use of public-private key cryptography ensures that a malicious user cannot have access to the system or an examination token that is not assigned to their identity. Performance evaluations indicate that the mean time for examination pass generation is 24.84 seconds and the average verification time for an examination pass at the point of admittance ranges between 3.91 seconds and 3.97 seconds. The results encompass a marked reduction in fraudulent activities, optimized pass issuance procedures, and heightened security for all involved parties.

Keywords:*Blockchain Technology, Examination Management, Hyperledger Fabric, Security*

INTRODUCTION

In this era where digital technology is rapidly advancing, various processes are starting to tilt towards electronic methods. Due to this, many organizations will need to modify their institutional frameworks to effectively embrace the rapid digital transformation, which holds significant potential for addressing the inherent limitations of conventional systems (Frizzo-Barker *et al*., 2020).

While adopting the contemporary approach of managing electronic documentation, most educational establishments still depend on manual procedures for the transfer of academic records, including transcripts, examination passes, and certificates (Badr*et al.*, 2019). Undoubtedly the educational institution is undergoing a digital transformation, and one crucial aspect of this evolution is the examination process. Traditionally, examinations have been administered in physical locations; requiring paper-based admission tickets also known as examination passes, and extensive administrative efforts. However, with the rapid advancement of technology, electronic examination management systems have gained prominence as a more efficient and scalable approach (Turkanovićet *al*., 2018).

It is worth noting that although comprehensive work has been done on blockchain-based entrance admission ticket systems, the framework of most of these solutions is designed to cater only to event entrance tickets such as concert tickets, and single-user tickets such as cafeteria tickets, flight tickets, movie tickets, etc. Single-user tickets refer to access passes or credentials that are issued to and intended for use by a specific individual. These tickets grant the holder the right to access a particular service, event, or location (Liu, 2021).

Examination passes can be classified as a form of entrance admission tickets, they function like single-user tickets, but there is a lot of contrast between examination passes and traditional single-user tickets and even standard entrance admission tickets such as concert tickets. One of the main differences is the framework that governs the issuance and verification of these electronic tickets, most single-user ticket systems are built on a public access architecture and are meant to provide ticketing services to the general public while examination passes are limited to use in a close environment specifically academic institutions and do not necessarily cater to the general public.

The major participants in an examination pass system are the examinees and the administrative body in charge of the examination process. However, it is important to note that while an examination pass shares similarities with traditional electronic single-user tickets, their underlying architecture may differ. In traditional electronic ticketing (e-ticketing) systems there is usually an issuing entity, the end-user, a collector, and a supplier that distributes it to the end-user after the issuing entity determines the content of a ticket (Rafati*et al.*, 2022).

Blockchain technology falls under the category of Distributed Ledger Technology (DLT) and operates as a distributed system (Liu, 2021). Within a distributed system, the process of attaining agreement among all nodes is referred to as the consensus algorithm and the Bitcoin blockchain employs the proof-of-work consensus algorithm. As new consensus algorithms emerge, they create new blockchain networks, branching from the original Bitcoin blockchain.

According to Peck (2017) and Wüst and Gervais (2018), while various blockchains rely on different consensus algorithms, they can be classified into two types based on the rules governing node participation in the network. The first type is the public blockchain, where anyone can opt to join the network as a node for reading, writing transactions, and mining new blocks, and can leave the network at will by relinquishing their nodes. The second type is the permissioned blockchain, which only permits specific designated participants to become nodes or join the network. Mingxiao*et al.* (2017) further categorize blockchains into three groups. Alongside public and permissioned blockchains, a form of private blockchain was introduced, characterized by centralization, where an owner wields ultimate authority over all the data. Since the educational system is a permissioned system most academic solutions that are blockchain-based are deployed on a permissioned blockchain such as Hyperledger Fabric (Guerreiro*et al.*, 2022). This reduces the potential for malicious attackers to gain access to the network.

While several solutions that have been proposed tend to provide modern methodologies for the digitalization and efficient management of academic assets, there are still several limitations in the areas of adoption, scalability, and real-time applications. Blockchain-based technologies could be of great benefit to Academic institutions as these blockchain-driven technologies offer a decentralized and immutable record to verify the authenticity of an examination pass. They establish an indelible history of academic records and procedures, facilitating validation by external parties without substantial manual effort and related expenses (Badr*et al*., 2019).

MATERIALS AND METHODS

This section sets out the methodologies and techniques employed in carrying out this research. The suggested framework was introduced and comprehensively scrutinized, encompassing its input and output parameters, state variables, and participants.

System Architecture and Mechanics

The system architecture in this research takes into consideration three major participants: an administrator, students and the invigilators. Several requirements are considered to ensure that the framework retains the advantages of the traditional examination pass system.

The framework was developed using Hyperledger fabric private blockchain. The architecture of the examination pass framework is depicted in Figure 1; it illustrates the internal network architecture the system uses to achieve decentralisation of data sharing whilst maintaining the security and privacy of participants. First, the network is initiated by the administrator which is the entity responsible for overseeing the governance of the examination pass system. Upon initiation of the network by the administrator, three distinct artifacts are established on the network: a network policy that provides the network initiator the administrative rights to govern the network in the form of a Membership Service Provider (MSP), a Certificate Authority (CA) which is responsible for assigning digital identities to permitted participants within the network and, an orderer node for ordering transactions into blocks before they are mined. After the network is initialized, the administrator creates additional channels for students and invigilators respectively. The students and invigilators do not need administrative rights hence their mode of operation is confined within the channels. Channels are segmented networks equipped with independent ledgers and smart contracts that enable members within the channel to exchange information amongst themselves. The student and invigilator channels are established with MSPs for students and invigilators alike. The administrator also creates a unique channel for itself to maintain a ledger of registered students, their identities, and examination pass information that can be shared with peer nodes on the student channel and invigilator channel without the need for administrative privileges.

Mechanics of the examination pass system

The system enables registered students with digital identities to request for examination pass using the front-end application. The front-end application can be in the form of a student portal allowing students to register on the blockchain by invoking the chain code deployed by the administrator. The system allows only students with assigned identities to request an examination pass within the stipulated period since the channel policy maintains their identities.

The student requests for the examination pass through the front-end application (along with a valid digital signature associated with their digital certificate), this request is validated via a chain code within the administrator peer node. The ledger of the student channel and the administrative channel is updated and records the examination pass as a transaction. The transaction contains the necessary information about the pass. The application for the invigilator is designed to be able to obtain student information and query the ledger through chain code maintained by its peer nodes to verify and validate if the exampass exists within the system.

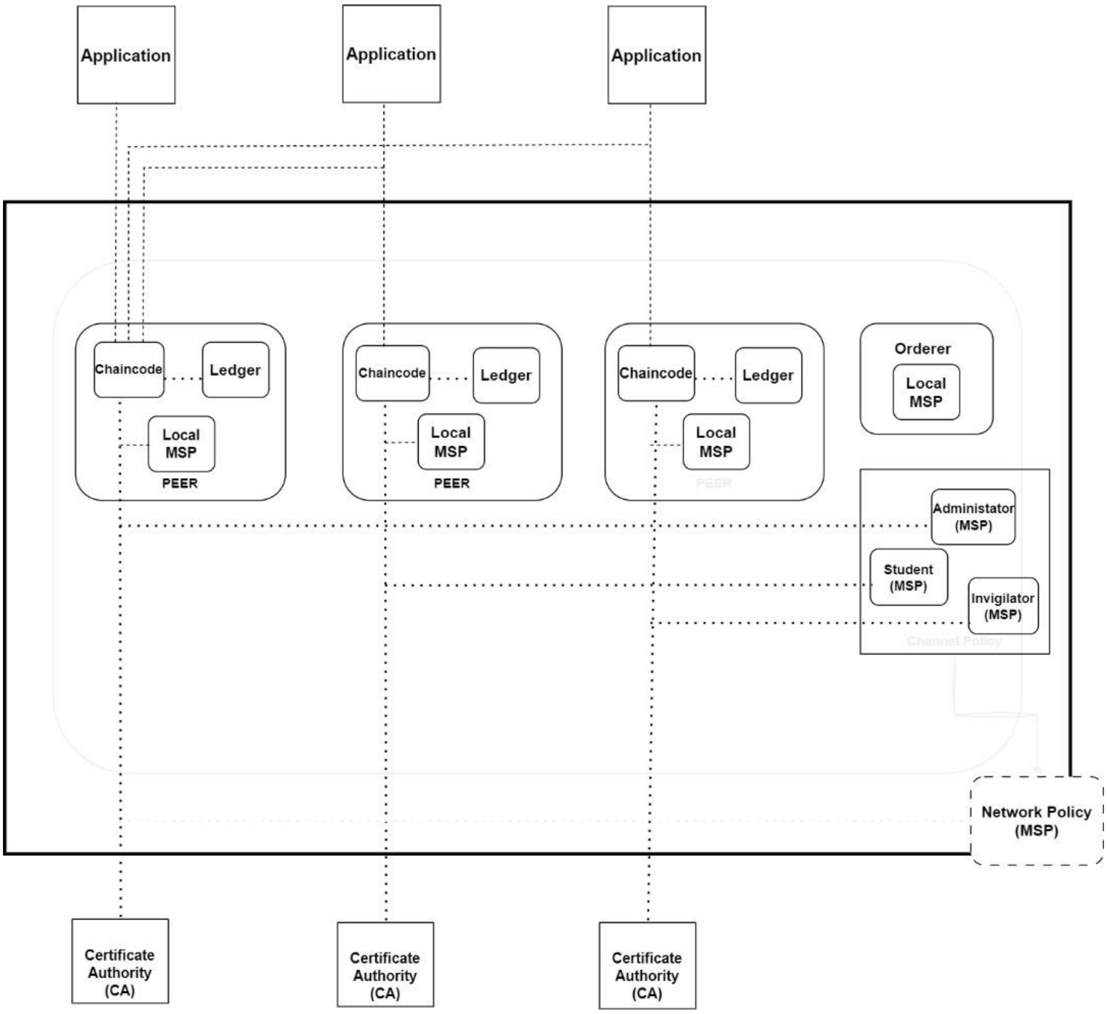


Figure 1: Network Architecture of the Examination Pass System

The flowchart in Figure 2 aims to achieve decentralisation of data sharing while maintaining the security and privacy of participants. The administrator plays a crucial role in initiating and governing the network, creating channels for students and invigilators, and managing the registration and assignment of digital identities for students.

System Implementation

The front-end application was developed using the React JS library. React is utilized for developing the front end because it can easily interact at the browser level with the MetaMask wallet which will enable the consumer to initiate a ticket purchase request and view a history of every ticket purchased by the specific consumer.

The Remix IDE was used to develop the ticketing smart contract and put it through different tests before being deployed to the sepolia test network for simulation.

Remix Integrated Development Environment (IDE) is an environment used to write, compile, test, and debug chain code using solidity. The decentralised ticketing model developed in this research work provides an improved approach to managing examination passes using blockchain technology. By leveraging Blockchain Technology and Solidity chain code, a secure, transparent, and decentralised model for managing examination passes that eliminates the need for a centralised ticketing provider, and reduces the risk of examination pass fraud is realized.

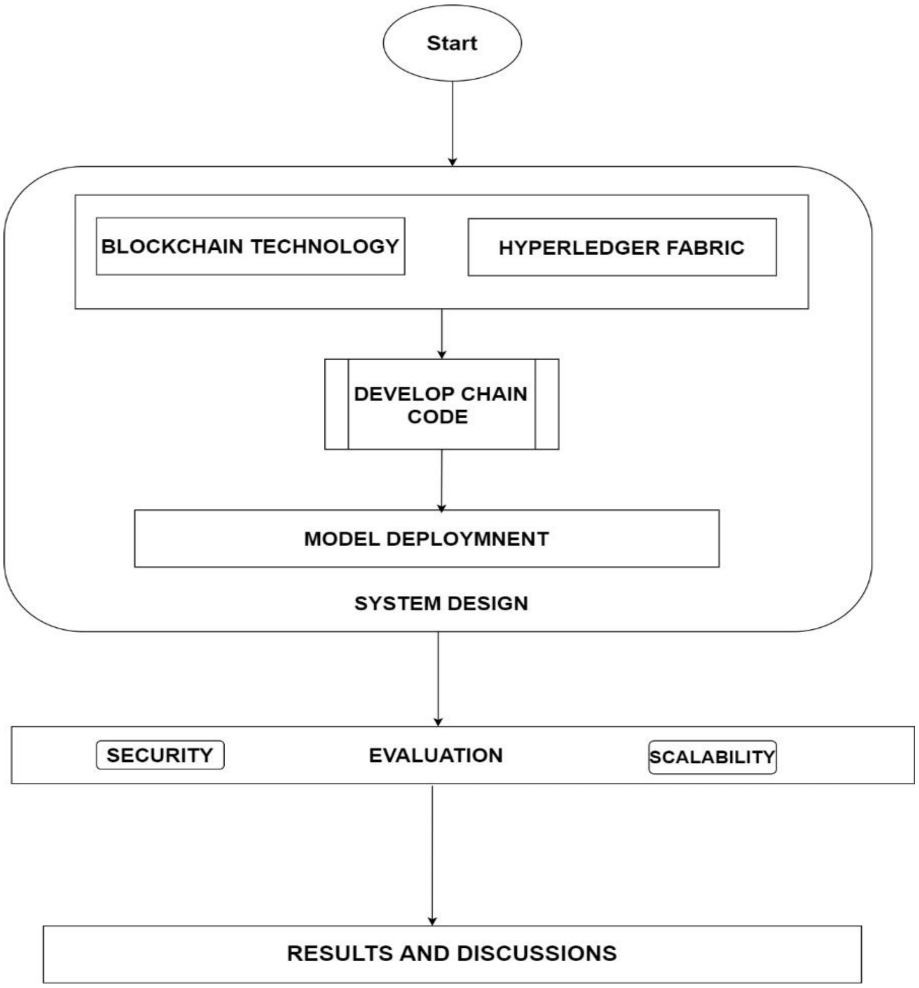


Figure 2**:** Flowchart of the Examination Pass System

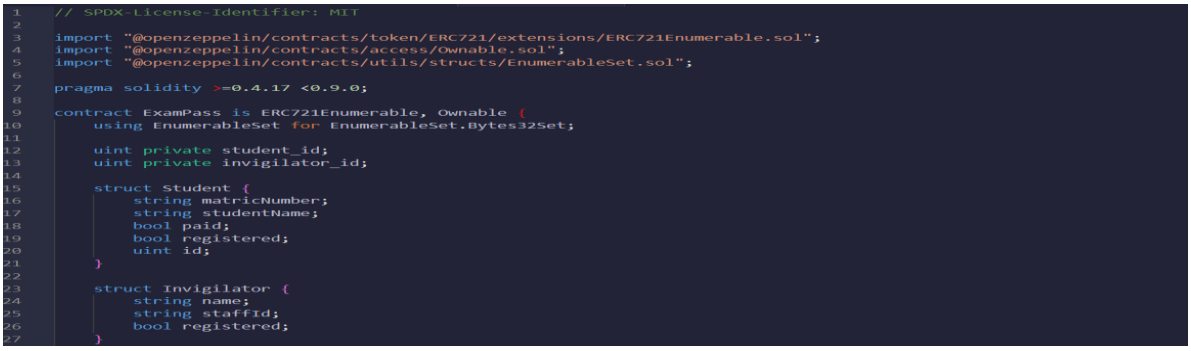
Data Functions for Examination Pass Chain Code

To enable students request an examination pass, only registered students who have paid the necessary fees will be able to request an examination pass successfully. The immutable nature of the blockchain network ensures that only users/students whose payment records have been updated on the blockchain can be able to call the **RequestExamPass**function which is used to create, encrypt and assign examination pass in the form of non-fungible tokens to the students' digital identity as seen in figure 4.

Figure 5 clearly shows the chain code that governs the student registration process. The function takes the student's name and matriculation number as input arguments.

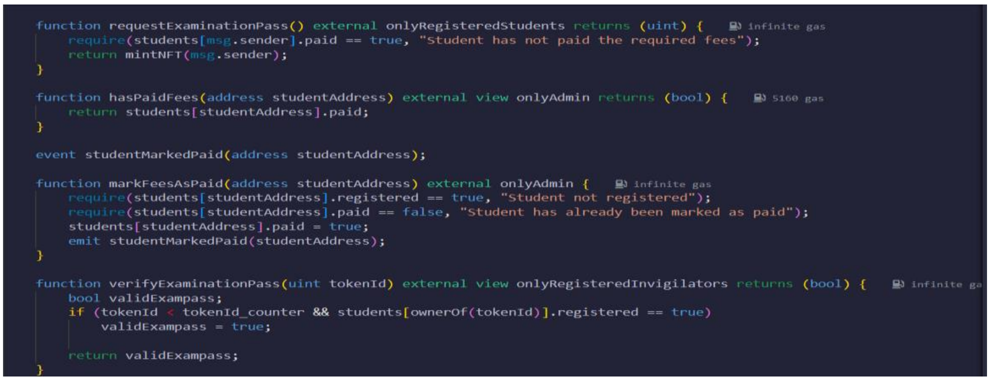
RESULTS AND DISCUSSION

The chaincode which is the backbone of the blockchain network was developed and tested in real time on the SepoliaTestnet. A comprehensive empirical analysis of the complete framework was carried out during testing, including information on its effectiveness at tracking and automating examination pass, security, reliability and traceability of examination pass information while ensuring consumer data is privet and secure.



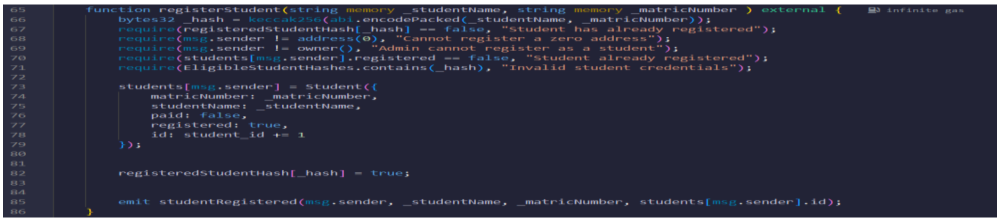
```
// SPDX-License-Identifier: MIT

import "@openzeppelin/contracts/token/ERC721/extensions/ERC721Enumerable.sol";
import "@openzeppelin/contracts/access/Ownable.sol";
import "@openzeppelin/contracts/utils/structs/EnumerableSet.sol";

pragma solidity >=0.4.17 <0.9.0;

contract ExamPass is ERC721Enumerable, Ownable {
    using EnumerableSet for EnumerableSet.Bytes32Set;

    uint private student_id;
    uint private invigilator_id;

    struct Student {
        string matricNumber;
        string studentName;
        bool paid;
        bool registered;
        uint id;
    }

    struct Invigilator {
        string name;
        string staffId;
        bool registered;
    }
```

Figure 3: Examination Pass Model Chaincode on Remix IDE



```
function requestExaminationPass() external onlyRegisteredStudents returns (uint) {
    require(students[msg.sender].paid == true, "Student has not paid the required fees");
    return mintNFT(msg.sender);
}

function hasPaidFees(address studentAddress) external view onlyAdmin returns (bool) {
    return students[studentAddress].paid;
}

event studentMarkedPaid(address studentAddress);

function markFeesAsPaid(address studentAddress) external onlyAdmin {
    require(students[studentAddress].registered == true, "Student not registered");
    require(students[studentAddress].paid == false, "Student has already been marked as paid");
    students[studentAddress].paid = true;
    emit studentMarkedPaid(studentAddress);
}

function verifyExaminationPass(uint tokenId) external view onlyRegisteredInvigilators returns (bool) {
    bool validExampass;
    if (tokenId < tokenId_counter && students[ownerOf(tokenId)].registered == true)
        validExampass = true;

    return validExampass;
}
```

Figure 4: Chaincode for enabling student to Request for Examination Pass



```
function registerStudent(string memory _studentName, string memory _matricNumber ) external {
    bytes32 _hash = keccak256(abi.encodePacked(_studentName, _matricNumber));
    require(registeredStudentHash[_hash] == false, "Student has already registered");
    require(msg.sender != address(0), "Cannot register a zero address");
    require(msg.sender != owner(), "Admin cannot register as a student");
    require(students[msg.sender].registered == false, "Student already registered");
    require(EligibleStudentHashes.contains(_hash), "Invalid student credentials");

    students[msg.sender] = Student({
        matricNumber: _matricNumber,
        studentName: _studentName,
        paid: false,
        registered: true,
        id: student_id += 1
    });


    registeredStudentHash[_hash] = true;


    emit studentRegistered(msg.sender, _studentName, _matricNumber, students[msg.sender].id);
}
```

Figure 5: Chaincode for governing Registration Process

Implementation Details

In implementing the model, the user interface for the decentralised application was designed, modeled, and prototyped using Figma. The openZeppelin ECDSA library was utilized to enable users to connect their wallet made up of their private and public key pair (generated using Elliptic Curve Cryptography) to the consumer client enabling a consumer to interact with the system by signing transactions, encrypting private data, and verifying ownership of assets on the network with the public-private key pair.

The hash of the student name and matriculation number is cross-checked on the database to verify if the student attempting to register is eligible to register on the system or has already been registered and if the bio-data presented during registration matches the student records maintained by the school. Figure 7 and Figure 8 depict the front-end representation of this function as tested in the Remix (IDE).

The function is a READ function so it takes the token encoded in the form of a QR (Quick Recovery) code and returns the validity status of the token and the details of the student assigned that particular examination token. Figure 9 shows the query result of an examination token generated by the token. Figure 9 clearly shows the result after a registered invigilator scans an exam token presented at the examination center and queries for the authenticity and validity of the exam token. The function returns the corresponding student details such as name, matriculation number, registration status and paid status.

Compiling and Deploying the Chaincode to the Blockchain Network

Before the chain code can be deployed to the blockchain, it has to be compiled to bytecode before it can be stored and run on the network. The solidity compiler 0.8.23+commit.87f61d96 was utilized for compilation. After the chaincode has been uploaded to the blockchain the software development kit invokes web3.js within its framework thereby enabling the front end of the decentralised application to interact with the blockchain network enabling participants to perform READ or WRITE operations to and from the chain code using Programming languages such as Python, ReactJS, GoLang and C++.

CONCLUSIONS

This research was carried out to develop a fully decentralized software model for electronic examination pass using blockchain technology. This research work helped in solving the problem of centralization in the issuance of examination pass which in most cases cannot be trusted.

The major advantage of this system is the implementation cryptographic algorithm which makes the blockchain immutable to intruders and the introduction of a real-time system during verification by the invigilator.

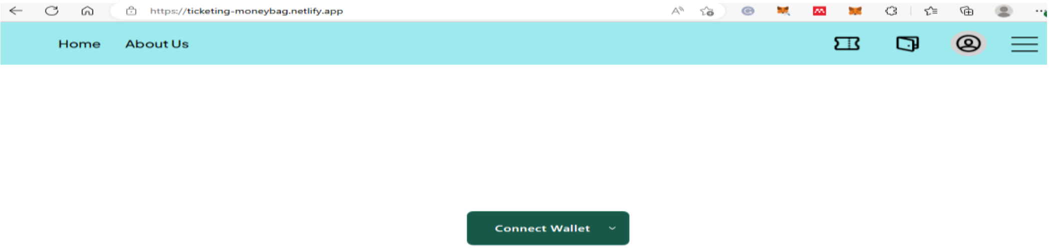
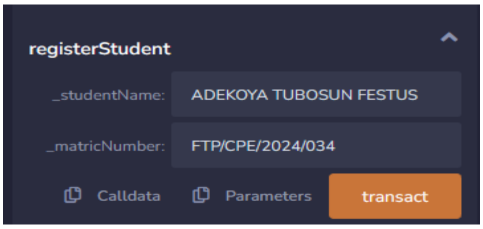


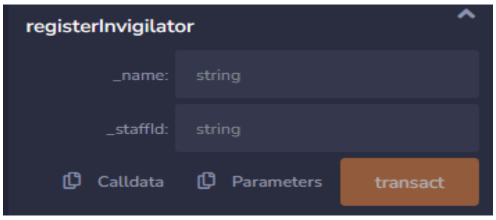
Figure 6: A screenshot of the login page of the model.


registerStudent

_studentName: ADEKOYA TUBOSUN FESTUS

_matricNumber: FTP/CPE/2024/034

Figure 7: Register Student

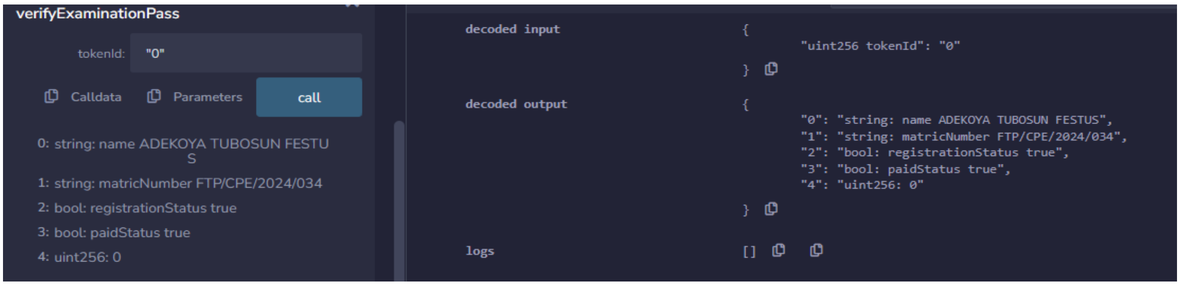

registerInvigilator

_name: string

_staffId: string

Figure 8: Register Invigilator

Figures 7 and 8**:** Showing the front-end application enabling student and invigilator registration

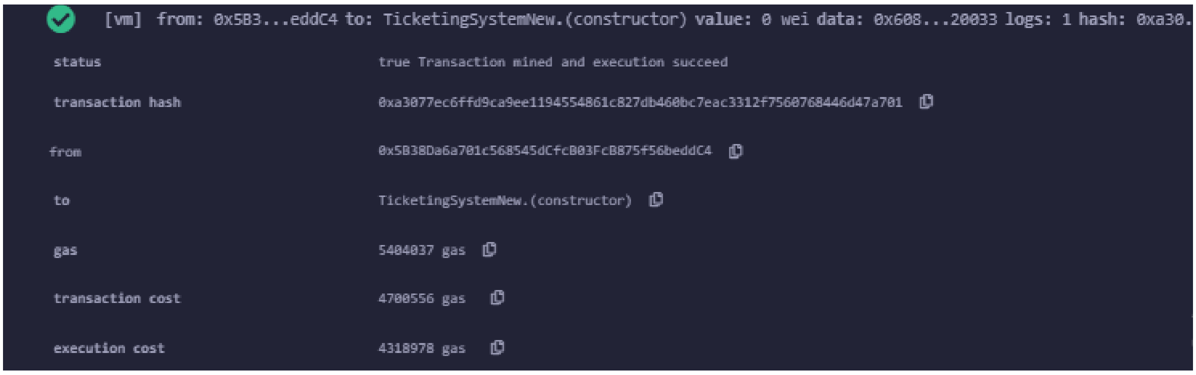


tokenId: "0"

```
0: string: name ADEKOYA TUBOSUN FESTU
S
1: string: matricNumber FTP/CPE/2024/034
2: bool: registrationStatus true
3: bool: paidStatus true
4: uint256: 0
```

```
decoded input        {
                         "uint256 tokenId": "0"
                     }
decoded output       {
                         "0": "string: name ADEKOYA TUBOSUN FESTUS",
                         "1": "string: matricNumber FTP/CPE/2024/034",
                         "2": "bool: registrationStatus true",
                         "3": "bool: paidStatus true",
                         "4": "uint256: 0"
                     }
logs                 []
```

Figure 9: Query result of an examination token on the blockchain



```
[vm] from: 0x5B3...eddC4 to: TicketingSystemNew.(constructor) value: 0 wei data: 0x608...20033 logs: 1 hash: 0xa30.
status                  true Transaction mined and execution succeed
transaction hash        0xa3077ec6ffd9ca9ee1194554861c827db460bc7eac3312f7560768446d47a701
from                    0x5B38Da6a701c568545dCfcB03FcB875f56beddC4
to                      TicketingSystemNew.(constructor)
gas                     5404037 gas
transaction cost        4700556 gas
execution cost          4318978 gas
```

Figure 10: Compilation results from Remix IDE

REFERENCES

Badr, A., Rafferty, L., Mahmoud, Q. H., Elgazzar, K., & Hung, P. C. K. (2019). A permissioned blockchain-based system for verification of academic records. *2019 10th IFIP International Conference on New Technologies, Mobility and Security, NTMS 2019 - Proceedings and Workshop*, 1–5. https://doi.org/10.1109/NTMS.2019.8763831.

Frizzo-Barker, J., Chow-White, P. A., Adams, P. R., Mentanko, J., Ha, D., & Green, S. (2020). Blockchain as a disruptive technology for business: A systematic review. *International Journal of Information Management*, *51*. https://doi.org/10.1016/j.ijinfomgt.2019.10.014.

Guerreiro, S., Ferreira, J. F., Fonseca, T., & Correia, M. (2022). Integrating an academic management system with blockchain: A case study. *Blockchain: Research and Applications*, *3*(4), 1–10. https://doi.org/10.1016/j.bcra.2022.100099.

Liu, M. (2021). *A Hybrid Blockchain-Based Event Ticketing System*. https://harvest.usask.ca/bitstream/handle/10388/13343/LIU-THESIS-2021.pdf?sequence=1&isAllowed=y.

RafatiNiya, S., Bachmann, S., Brasser, C., Bucher, M., Spielmann, N., & Stiller, B. (2022). DeTi: A Decentralized Ticketing Management Platform. *Journal of Network and Systems Management*, *30*(4). https://doi.org/10.1007/s10922-022-09675-3.

Turkanović, M., Hölbl, M., Košič, K., Heričko, M., &Kamišalić, A. (2018). EduCTX: A blockchain-based higher education credit platform. *IEEE Access*, *6*, 5112–5127. https://doi.org/10.1109/ACCESS.2018.2789929.