Project Report

on

Blockchain Based Educational Records Storage and Sharing

Submitted by

BADIGINCHALA CHANDANA PRIYA-(20BCS026)

KOTHA BALAJI-(20BCS073)

LALAM DIVYA SRI-(20BCS076)

NAGELLA PRANAV REDDY-(20BCS089)

Under the guidance of

Dr. Rajendra H

Head of department DSAI

Dharwad
ज्ञानेन विकासः

INDIAN INSTITUTE OF
INFORMATION
TECHNOLOGY

INDIAN INSTITUTE OF INFORMATION TECHNOLOGY DHARWAD

Contents

List of Figures

1 Introduction

The education system relies heavily on records to verify credentials, academic achievements, and other important information. Traditionally these records are stored as paper physical records. Later with the development of Information Technology (IT), educational records have been digitized. These digital records are stored on the storage medium which has a high degree of variability, which means that these records can be easily modified during the process of storage, transmission and sharing. The traditional record-keeping systems are often plagued by issues of:

1. Fraud
2. Data tampering
3. Accessibility

Blockchain technology has the potential to address all these challenges and provide a more secure and transparent way to store and share educational records. It provides a range of benefits, such as reducing administrative costs, minimizing fraud and identity theft, improving data accuracy, and simplifying the verification process for educational institutions and employers.

1.1 Problem Statement

” Accurate and complete educational records are a valuable asset for people. Over the years, educational records have been digitized. But there are two major problems that have not been overcome. One is to achieve reliable and privacy-preserving storage of educational records, while another is how to understand the sharing of educational records and ensure the protection of the process of sharing.”

2 Related Work

In recent years, blockchain technology has gained significant popularity and has been widely adopted as the underlying framework for cryptocurrencies like Bitcoin [1].

The authors of [2] and [3] have proposed secure data storage solutions in the power energy field using blockchain technology to enhance the protection of energy data against cyber-attacks. Similarly, in transportation and supply chain management, blockchain technology can also be employed [4]. Traditional centralized electric vehicle charging systems are susceptible to Distributed Denial of Service (DDoS) attacks on the central charging server. To address this issue, a blockchain-based charging system has been suggested, offering key security, secure mutual authentication, and efficient charging. In [5], the authors have utilized smart contracts on the blockchain to assess the credibility of crowdsourced data and ensure safe and efficient traffic operations, eliminating the need for a single authority and presenting a secure real-time traffic event detection solution. Additionally, research has been conducted to enhance the security and reliability of communication data within vehicle networks [6], [7].

The Massachusetts Institute of Technology (MIT) has developed a system called ”Blockcerts Wallet” that serves as a platform for building blockchain-based applications. This system focuses on issuing and verifying official records, enabling the creation of a certificate wallet for students to receive virtual diplomas through their smart devices [8]. While similar in the goal of facilitating the creation and dissemination of educational records using blockchain, Blockcerts Wallet differs from the Blockchain-based Educational Records Repository (BcER2) as it is primarily an application development platform.

The other application of blockchain technology is the concept of ”intelligent contracts.” Ethereum, a blockchain platform discussed in [9], allows for the creation of self-managed contracts. These contracts are triggered by predefined events, such as the expiration of a date or the achievement of a specific price goal. The smart contract then autonomously adjusts itself as needed without requiring external input or intervention from third parties.

3 System Design and Architecture

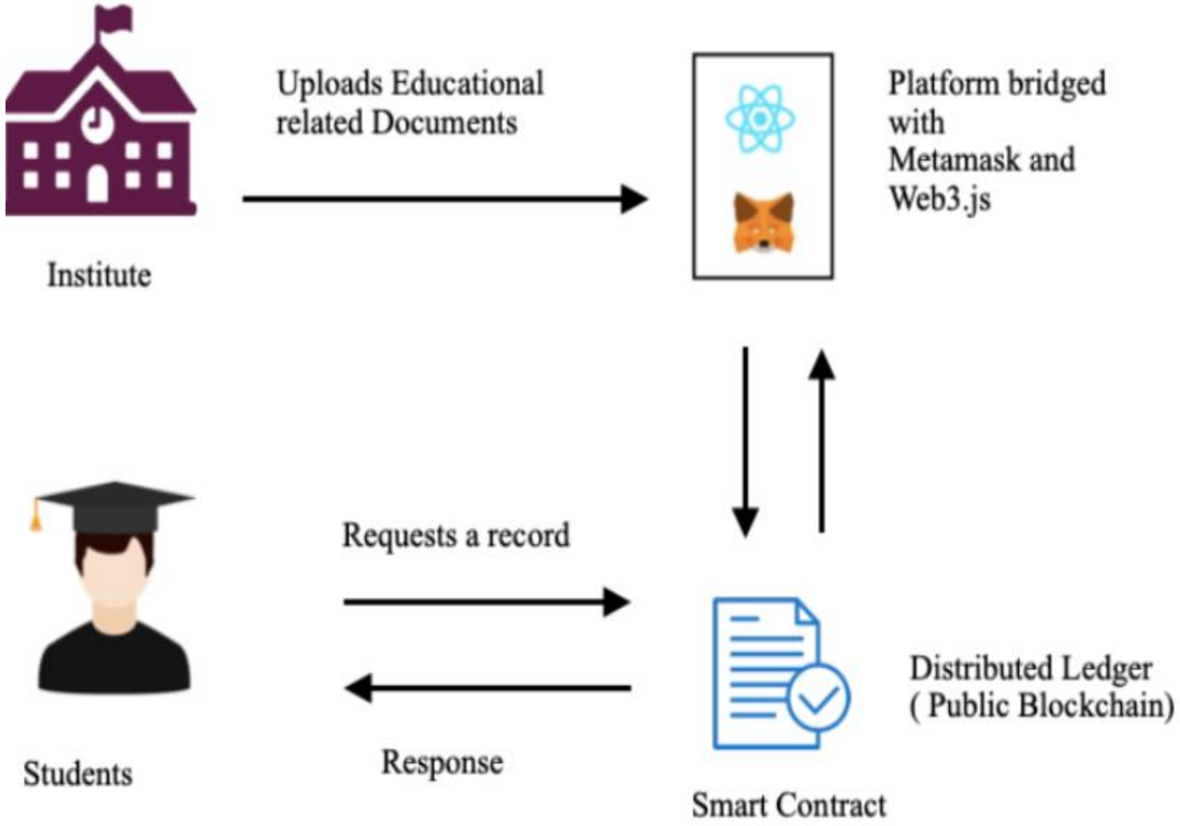

Uploads Educational related Documents
Platform bridged with Metamask and Web3.js
Institute
Requests a record
Students
Response
Distributed Ledger (Public Blockchain)
Smart Contract

Figure 1. System Design and Architecture

4 Methodology

- Requirement gathering: we have conducted a search on existing solutions of our project, and we have analyzed their strengths, weaknesses, and limitations.

- Developing the system: Build the system, including the smart contracts, backend infrastructure, and frontend applications.

- Testing and validation: Conduct rigorous testing and validation of the system to ensure itsfunctionality, security, and scalability.

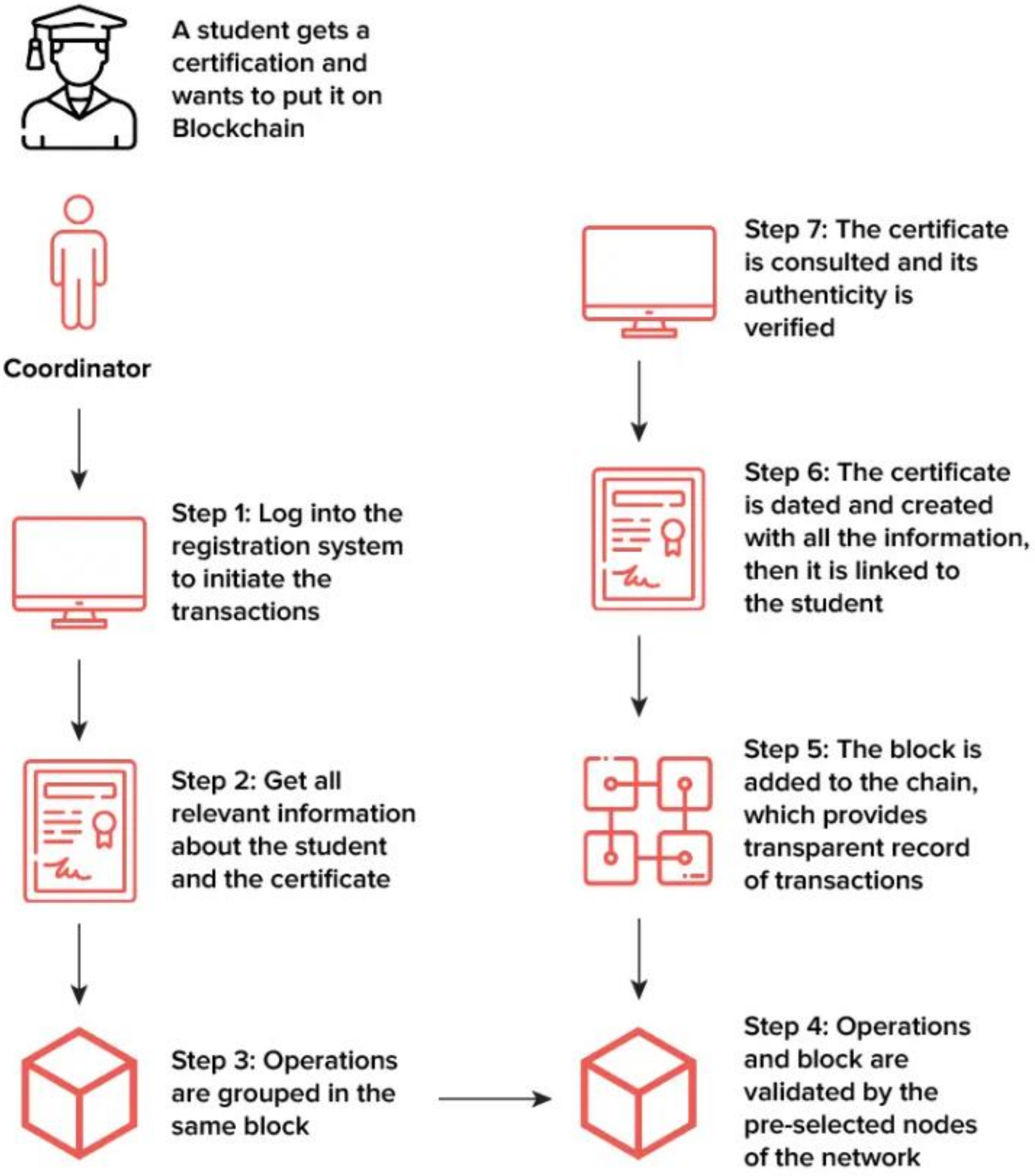

A student gets a certification and wants to put it on Blockchain
Coordinator
Step 1: Log into the registration system to initiate the transactions
Step 2: Get all relevant information about the student and the certificate
Step 3: Operations are grouped in the same block
Step 4: Operations and block are validated by the pre-selected nodes of the network
Step 5: The block is added to the chain, which provides transparent record of transactions
Step 6: The certificate is dated and created with all the information, then it is linked to the student
Step 7: The certificate is consulted and its authenticity is verified

Figure 2. Methodology

5 Technology used

- Blockchain:
  - Ethereum
  - Web3
  - Solidity
  - IPFS
  - Ganache
- Front End (Web DApp)
  - React JS
  - CSS
  - Bootstrap
- Back End
  - NodeJS
- Hosting Services
  - Metamask

6 Smart contracts Description

1. FileContract:
This contract specifies the "File" structure, which stands for a file that is kept on the blockchain. It contains details like the file hash, filename, description, and owner address. The contract offers an upload function that requires the file hash, description, and address of the uploader. Each file is individually identified by its owner's address and file count, which are saved in a mapping named "files" that stores the files. When a file is uploaded, the event "FileCreated" is released. A function to retrieve a file's filename based on the owner's address and file number is also available.

2. FileTransfer:
With this contract, IPFS (InterPlanetary File System) addresses are allowed to be transferred between addresses. For each address, it has a mapping called "ipfsInbox" that stores an IPFS address. A function to deliver an IPFS address to a specific address is provided by the contract. Before transmitting a new IPFS address, the modifier "notFull" ensures that the recipient's inbox is empty.

When an IPFS address is sent or the inbox is checked, the events "ipfsSent" and "inboxResponse" are emitted, respectively.

3. SchoolContract:

This contract handles school-related functionality and interacts with UserContract, FileContract, and StudentContract. It includes mappings to store students' information and their corresponding school addresses. The contract provides functions to add students, check if a student exists, get student information, and retrieve students associated with a school address. It also keeps track of student records using an array and a mapping. The constructor takes addresses of FileContract and StudentContract to establish connections with them.

4. UserContract:

This contract controls user-related functions. It establishes a structure called "User" to hold user data such as email address, first and last name, school address, and name. The agreement has a mapping called "users" for storing user data based on addresses. By entering the school address, the user address, and the user details, a user can be created. The user's name can also be retrieved using a function that uses the user's address.

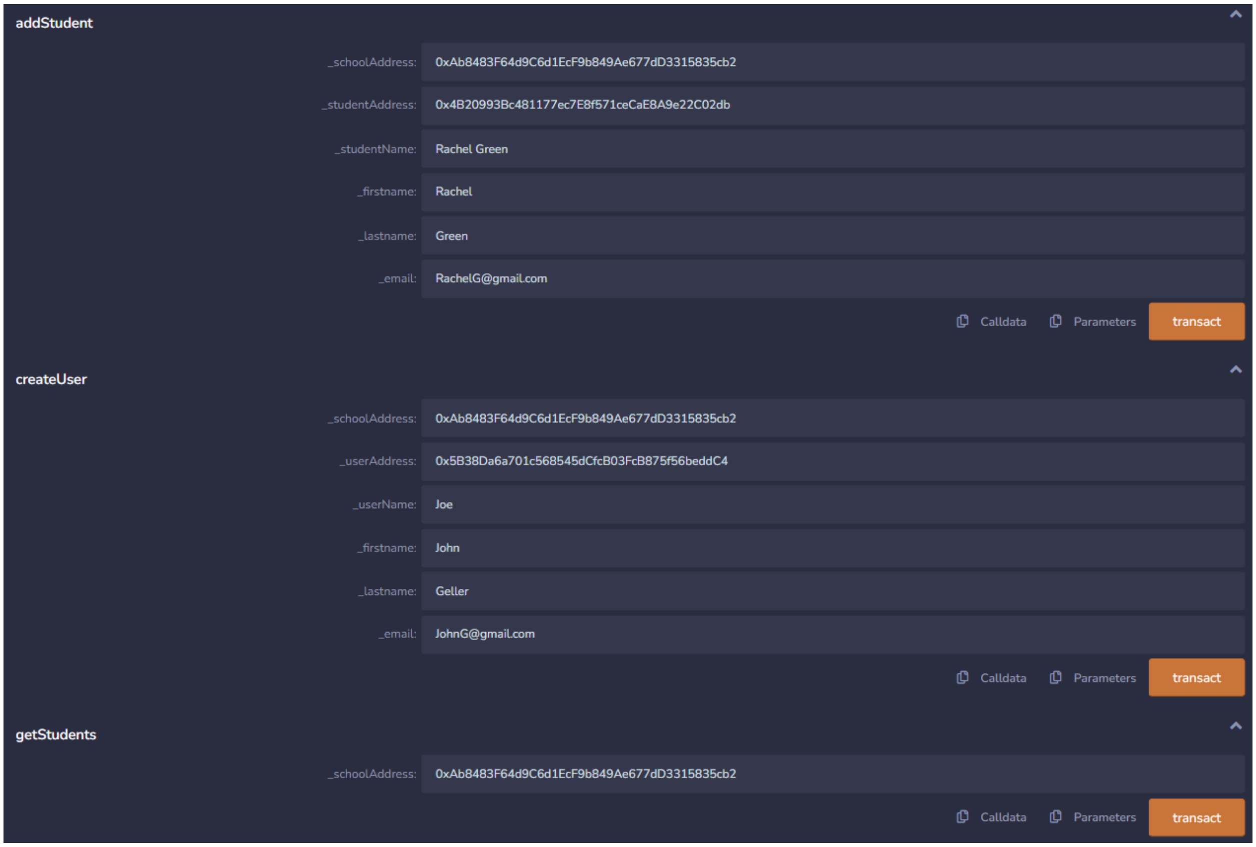
5. StudentContract:

This contract extends the functionality of UserContract and interacts with FileContract. It includes a reference to FileContract. The constructor takes the address of FileContract to establish a connection. The contract provides functions related to student information and file ownership. However, the specific functions mentioned in the comments, such as "getFile" and "fileCount," are not implemented in the provided code.

7 Experimental Results

We used remix.ethereum.org for compiling and deploying our project smart contracts. The following are the results of the smart contracts:

1. SCHOOL CONTRACT FUNCTION RESULTS:



addStudent

_schoolAddress: 0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2

_studentAddress: 0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db

_studentName: Rachel Green

_firstname: Rachel

_lastname: Green

_email: RachelG@gmail.com

createUser

_schoolAddress: 0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2

_userAddress: 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4

_userName: Joe

_firstname: John

_lastname: Geller

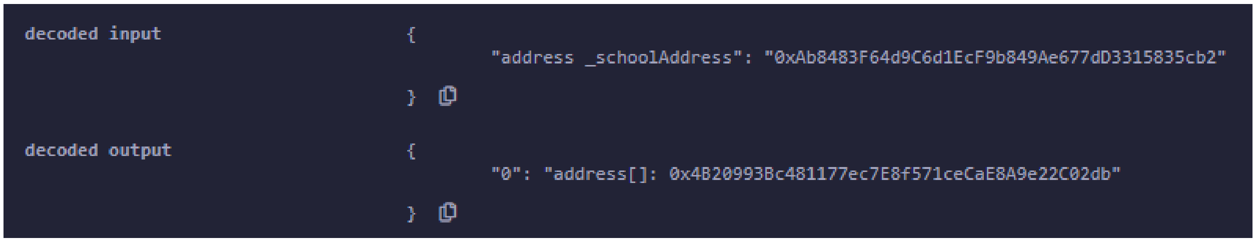
_email: JohnG@gmail.com

getStudents

_schoolAddress: 0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2

Figure 3. School contract result-1

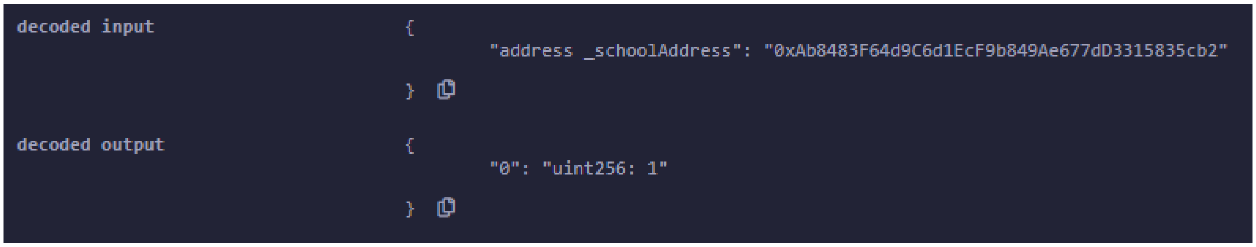
Here, firstly we have created a user of a school with the respective credentials as shown above, then added a student to the created school, to get the students in that school we have a function to access it that is “geStudents” also the school can keep tracts of number of students in their organization by the function “studentCount”. The two pictures below show this result:



```
decoded input                  {
                                       "address _schoolAddress": "0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2"
                               }

decoded output                 {
                                       "0": "address[]: 0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db"
                               }
```

Figure 4. School contract result-2

Here, decoded input holds the school address and the decoded output holds the address of the associated student.



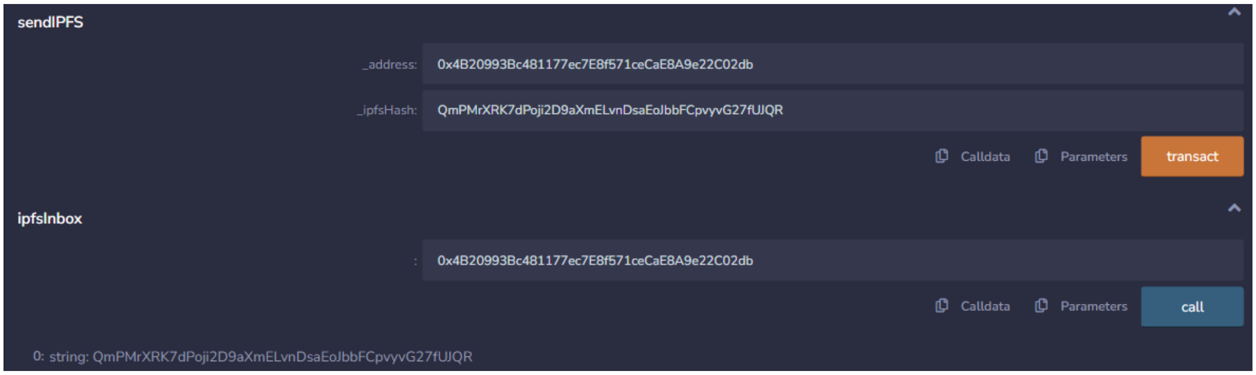
```
decoded input                  {
                                       "address _schoolAddress": "0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2"
                               }

decoded output                 {
                                       "0": "uint256: 1"
                               }
```

Figure 5. School contract result-3

As we have added one student the output shows as 1 which represents the student count for the given school address.

2. FILE TRANSFER FUNCTION RESULTS:

For transferring the file, we use sendIPFS function in which we give the receiver address and the file hash that we got from IPFS for the required file. And the receiver can check their inbox to see the file hash that they have received. The below figure shows the results of this process:



sendIPFS

_address: 0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db

_ipfsHash: QmPMrXRK7dPoji2D9aXmELvnDsaEoJbbFCpvyvG27fUJQR

ipfsInbox

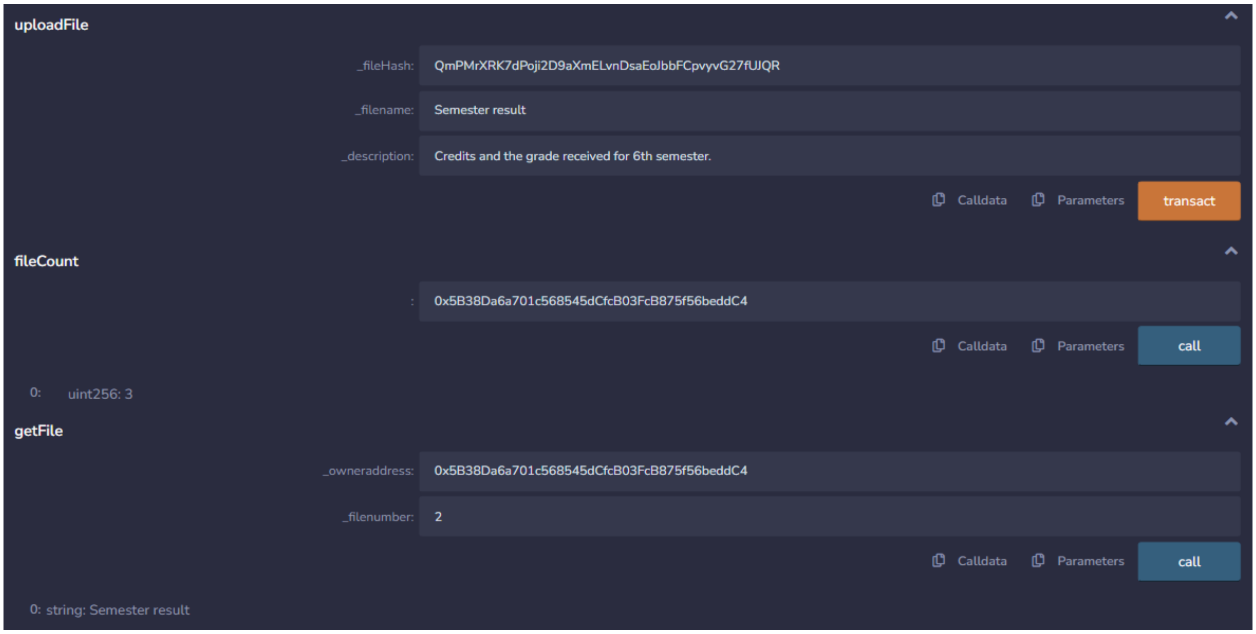
: 0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db

0: string: QmPMrXRK7dPoji2D9aXmELvnDsaEoJbbFCpvyvG27fUJQR

Figure 6. File transfer result

3. FILE CONTRACT FUNCTION RESULTS:

The valid or authenticated user of the contract can upload the files to their respective address. And we have used this contract in both the student and school contracts so that they have an option to store their own files to their own address.



uploadFile

_fileHash: QmPMrXRK7dPoji2D9aXmELvnDsaEoJbbFCpvyvG27fUJQR

_filename: Semester result

_description: Credits and the grade received for 6th semester.

fileCount

: 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4

0: uint256: 3

getFile

_owneraddress: 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4

_filenumber: 2

0: string: Semester result

Figure 7. File Contract result

8 Challenges

Blockchain technology has the potential to revolutionize the way educational records are stored and shared. It can offer a secure, transparent, and decentralized way of storing and sharing educational records. However, there are still some challenges that need to be addressed before blockchain-based educational records storage and sharing become widely adopted.

Privacy: Ensuring the protection and confidentiality of personal and sensitive information stored in educational records.

Interoperability: Enabling seamless exchange and access of educational records across different systems and institutions.

Access: Providing authorized individuals with the ability to access and view relevant educational records while maintaining data security and privacy.

Verification and Validation: Establishing the authenticity, integrity, and accuracy of educational records through processes of verification and validation to ensure their trustworthiness and reliability.

9 Future Scope

In the future, we hope to deploy the blockchain-based educational records secure storage and sharing system in a production environment, where we will closely evaluate its performance, security, and scalability. By regularly monitoring performance and also by addressing any potential vulnerabilities, we can make sure that the system is secure and operating efficiently. Additionally, we also consider the user feedback with the goal of boosting its performance, security, and usability, and improve any required upgrades to the system’s user interface. We also think about integrating the system with any external services, and we'd like to stay on top of the most recent advancements in blockchain technology. We also think about creative ways to enhance the system's efficiency, security, and scalability. We intend to create a strong, dependable, and simple solution for educational institutions that will safeguard the integrity and confidentiality of student records.

10 Conclusion

The use of blockchain technology for educational records storage and sharing offers secure and transparent solutions. It ensures the integrity and security of data through consortium chains and distributed institution authentication. Smart contracts facilitate cross-institutional sharing of records while maintaining permissions and managing the sharing process. The combination of blockchain and storage servers enables efficient storage, while smart contracts manage permissions and facilitate cross-institutional sharing. Future research should focus on secure platform development, expanded functionalities, and exploring decentralized storage options. Blockchain-based educational records storage and sharing hold great potential for transforming current systems, offering higher security, efficiency, and credibility.

References

[1] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system
https://bitcoin.org/bitcoin

[2] C. Pop, M. Antal, T. Cioara, I. Anghel, D. Sera, I. Salomie, G. Raveduto, D. Ziu, V. Croce, and M. Bertoncini, "Blockchain-based scalable and tamper-evident solution for registering energy data".
https://www.mdpi.com/1424-8220/19/14/3033

[3] G. Liang, S. R. Weller, F. Luo, J. Zhao, and Z. Y. Dong, "Distributed blockchain-based data protection framework for modern power systems against cyber attacks," IEEE Trans.
https://ieeexplore.ieee.org/document/8683437

[4] M. Kim, K. Park, S. Yu, J. Lee, Y. Park, S.-W. Lee, and B. Chung, "A secure charging system for electric vehicles based on blockchain".
https://www.mdpi.com/1424-8220/19/13/3028

[5] J. Mihelj, Y. Zhang, A. Kos, and U. Sedlar, "Crowdsourced traffic event detection and source reputation assessment using smart contracts" .
https://www.mdpi.com/1424-8220/19/15/3267

[6] Z. Yang, K. Zheng, K. Yang, and V. C. M. Leung, "A blockchain-based reputation system for data credibility assessment in vehicular networks," in Proc.
https://ieeexplore.ieee.org/document/8292695

[7] G. Rathee, A. Sharma, R. Iqbal, M. Aloqaily, N. Jaglan, and R. Kumar, "A blockchain framework for securing connected and autonomous vehicles".
https://www.mdpi.com/1424-8220/19/14/3165

[8] MIT Media Lab. (n.d.). Blockcerts: An open standard for blockchain credentials.
https://www.blockcerts.org/

[9] Buterin, V. (2013). Ethereum whitepaper: A next-generation smart contract and decentralized application platform.
https://ethereum.org/en/whitepaper/

[10]Hongzhi Li And Dezhi Han, “EduRSS: A Blockchain-Based Educational Records Secure Storage and Sharing Scheme”.
https://ieeexplore.ieee.org/document/8915819