Secure sharing of Students' Credentials

Group Details:

1. Ashish Asthana - 2018A7PS0239P
2. Apoorv Sadana - 2018A7PS0165P

Assumptions and Objectives of the Project:

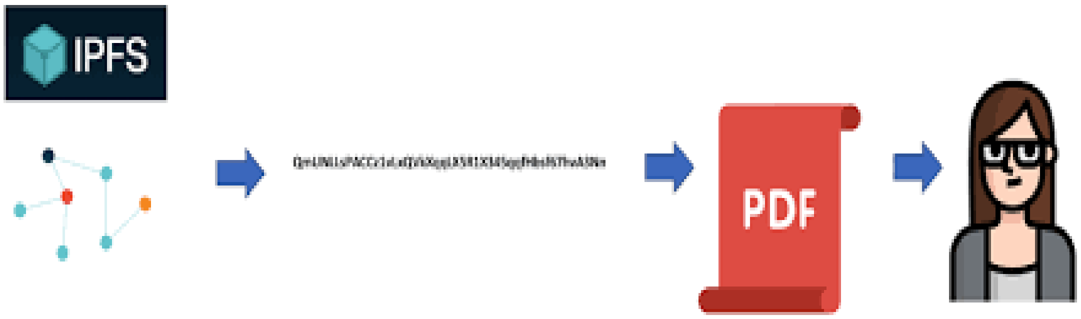
Student credentials are documents pivotal to all the enrolled institutes throughout life as well as the government, employing firms and research programs. To ensure the security of these documents the current system has Digi-locker availabilities, ERP logins and the rest just provide hard copies of the documents. These documents need to be verified by institutions students are applying to. Security of these documents is of utmost importance considering the value held by these. We believe no implementation of such a solution is available publicly. A research paper discusses this approach but no code is available for the same. We assume that a faster, more secure, more robust solution for handling these academic documents is required as well as the elimination of any manual process. We aim to eliminate the day's long processes for gaining access to these documents, to enhance the security of such a system as these are incredibly important and confidential documents and integrate it for ease of schools to provide such documents, students to view and own these documents and for companies to gain access to these documents.

Technical concepts not taught in class:

IPFS

IPFS is the acronym for Interplanetary File System. It's a project that aims to provide a step closer to a truly decentralized Internet. In today's Internet most of the data, images, files, videos, etc. are stored on database farms that are mainly owned by big companies. This is a typical centralization scenario and thus also suffers from the issues of centralization. These documents are hence not censorship-free and can be regulated by the database owners, governments and other authorities. Apart from this these databases act as a single point of failure so once it fails that file is lost from the server. It is also possible for malicious agents to modify and access it and it's also not immutable. IPFS aims to overcome all these shortcomings in the following manner. It operates over a P2P network. A file in the current Internet is addressed via a URL. However in IPFS, the file is content-addressable, what this means is that a file with certain content is given a unique IPFS hash and the file is accessed via this hash. P2P network gives the decentralized aspect as a file is likely to be available at multiple peers. This eliminates the single point of failure problem. The file is also tamper-resistant and immutable as if the contents of a file is changed then its hash would also be changed and we can detect this by comparing it with the original hash. Further, it cannot be censored because there's no single central authority in this system.

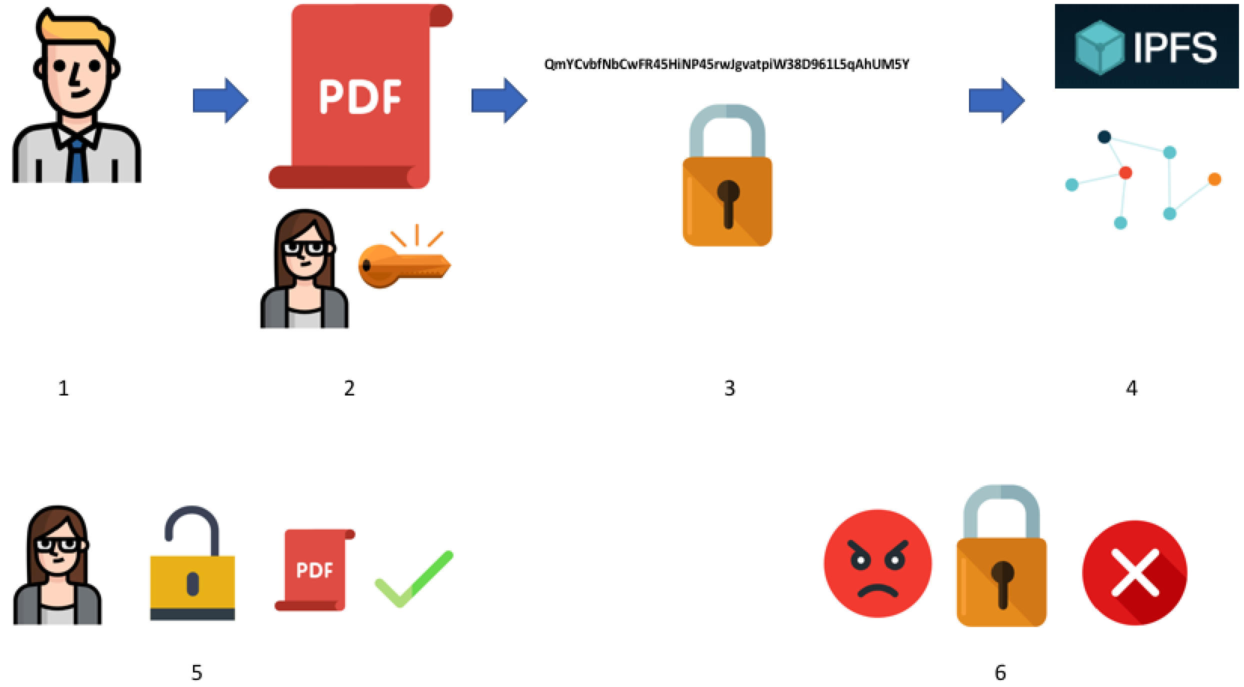
IPFS Document Access Process:



IPFS P2P NETWORK => FILE CONTENT ADDRESSABLE HASH => FILE => USER

IPFS Document Uploading Process:

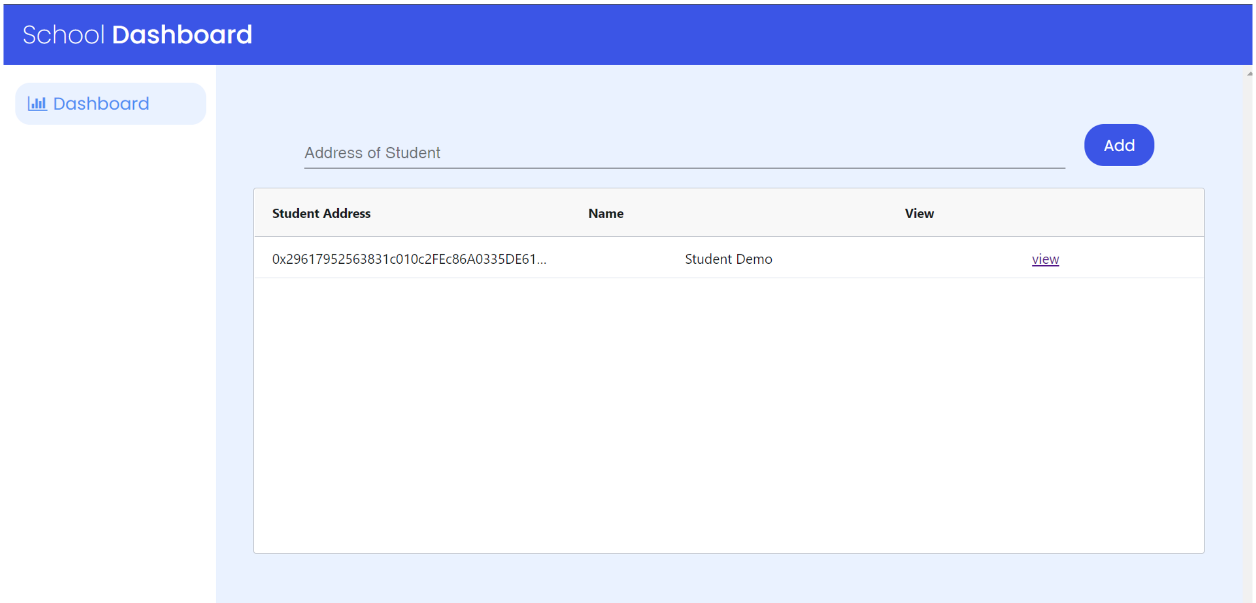
USER => FILE => FILE CONTENT ADDRESSABLE HASH => IPFS P2P NETWORK



Working of Project:

School Dashboard

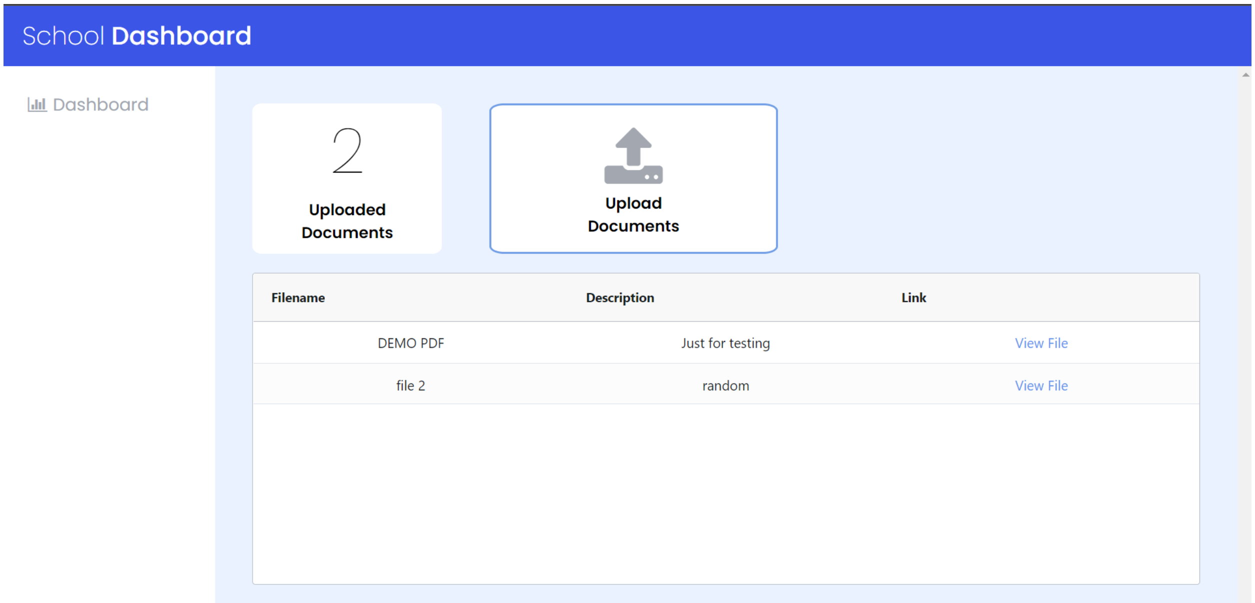
You can add students to the school and also view existing students within the school



Address of Student

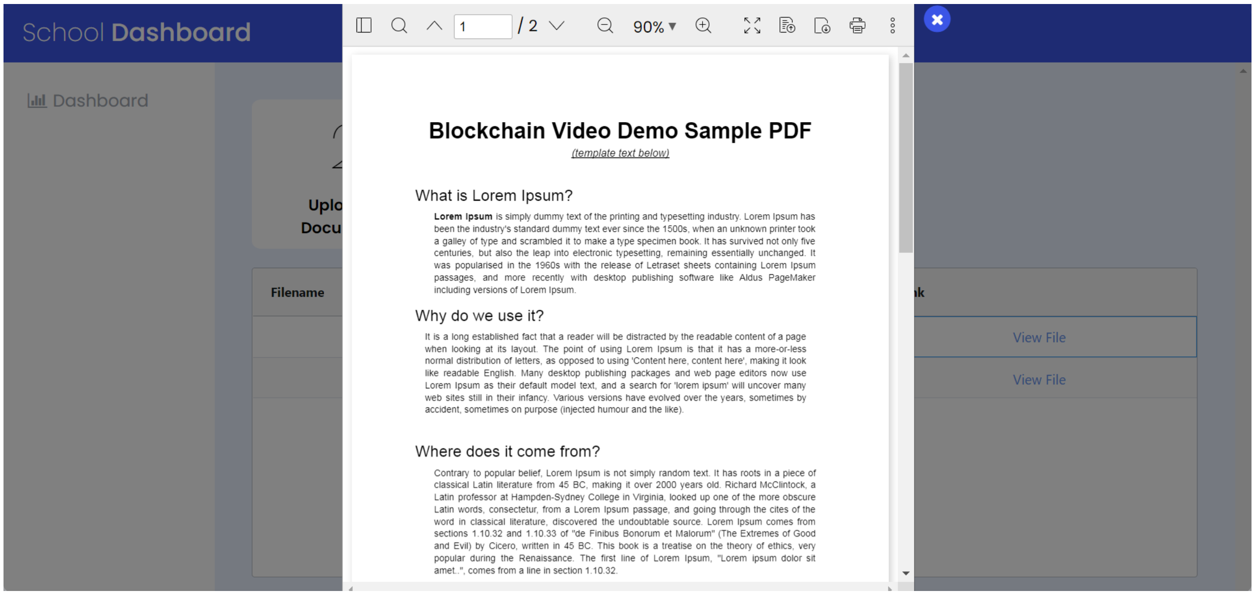
Student Address	Name	View
0x29617952563831c010c2FEc86A0335DE61...	Student Demo	view

Clicking on the **view** above, you can see all the files of the student



Filename	Description	Link
DEMO PDF	Just for testing	View File
file 2	random	View File

Clicking on **View File** will open a new tab with the ipfs link of the file. In case of PDF, the file can be seen on the frontend as well



Blockchain Video Demo Sample PDF

(template text below)

What is Lorem Ipsum?

Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book. It has survived not only five centuries, but also the leap into electronic typesetting, remaining essentially unchanged. It was popularised in the 1960s with the release of Letraset sheets containing Lorem Ipsum passages, and more recently with desktop publishing software like Aldus PageMaker including versions of Lorem Ipsum.

Why do we use it?

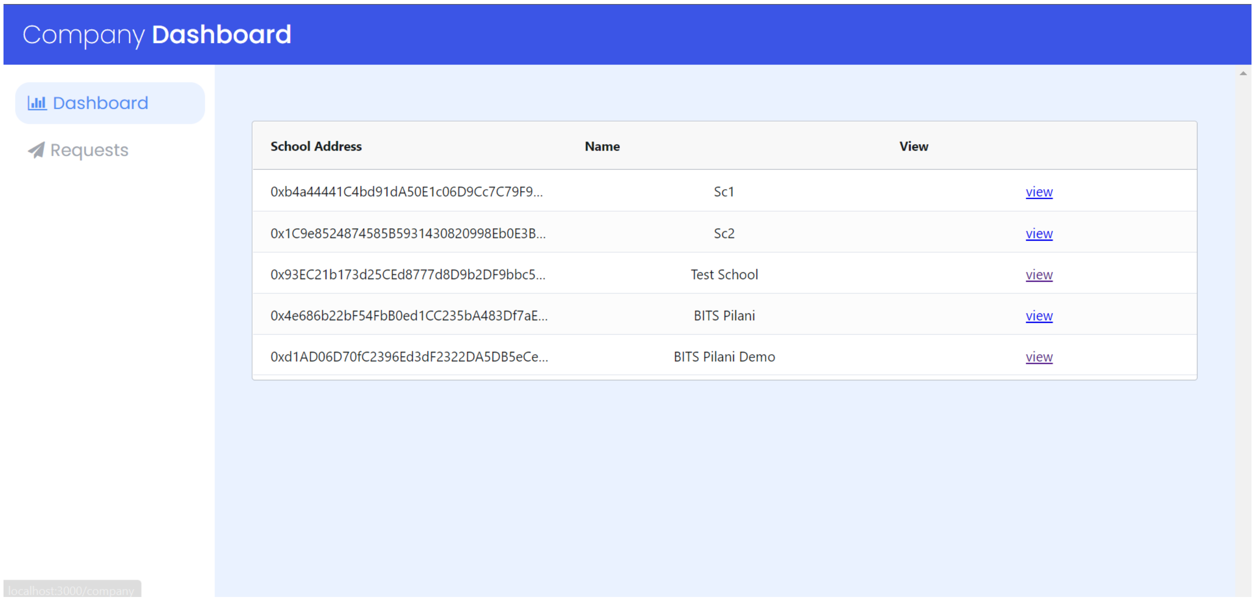
It is a long established fact that a reader will be distracted by the readable content of a page when looking at its layout. The point of using Lorem Ipsum is that it has a more-or-less normal distribution of letters, as opposed to using 'Content here, content here', making it look like readable English. Many desktop publishing packages and web page editors now use Lorem Ipsum as their default model text, and a search for 'lorem ipsum' will uncover many web sites still in their infancy. Various versions have evolved over the years, sometimes by accident, sometimes on purpose (injected humour and the like).

Where does it come from?

Contrary to popular belief, Lorem Ipsum is not simply random text. It has roots in a piece of classical Latin literature from 45 BC, making it over 2000 years old. Richard McClintock, a Latin professor at Hampden-Sydney College in Virginia, looked up one of the more obscure Latin words, consectetur, from a Lorem Ipsum passage, and going through the cites of the word in classical literature, discovered the undoubtable source. Lorem Ipsum comes from sections 1.10.32 and 1.10.33 of "de Finibus Bonorum et Malorum" (The Extremes of Good and Evil) by Cicero, written in 45 BC. This book is a treatise on the theory of ethics, very popular during the Renaissance. The first line of Lorem Ipsum, "Lorem ipsum dolor sit amet..", comes from a line in section 1.10.32.

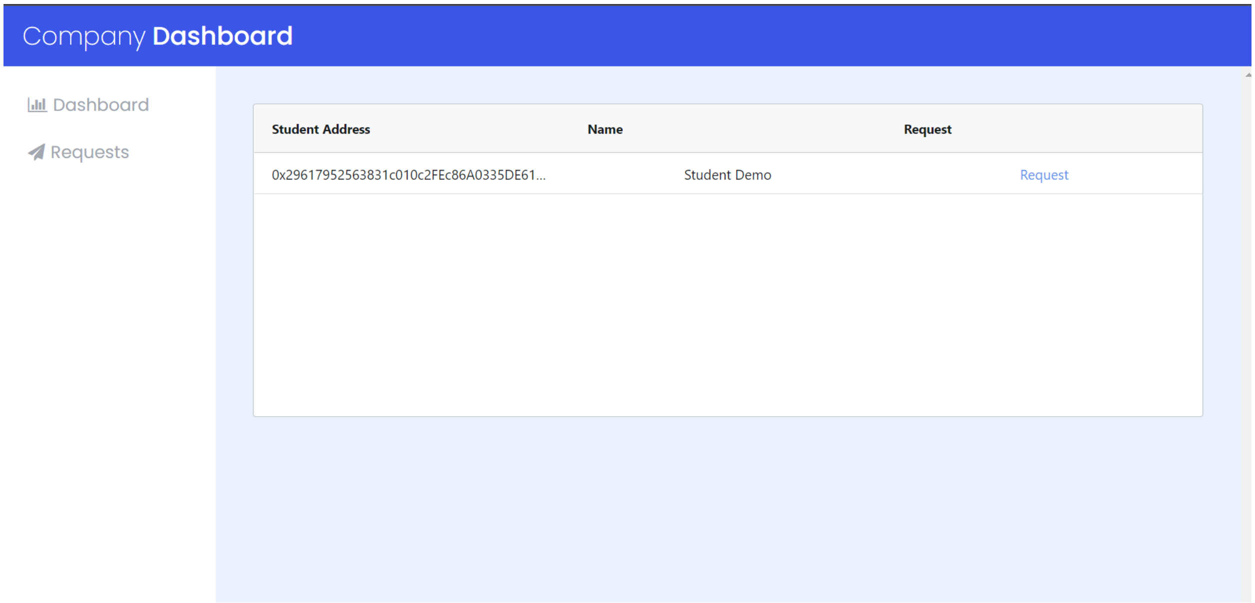
Company Dashboard

On the main dashboard, you can see all the registered schools



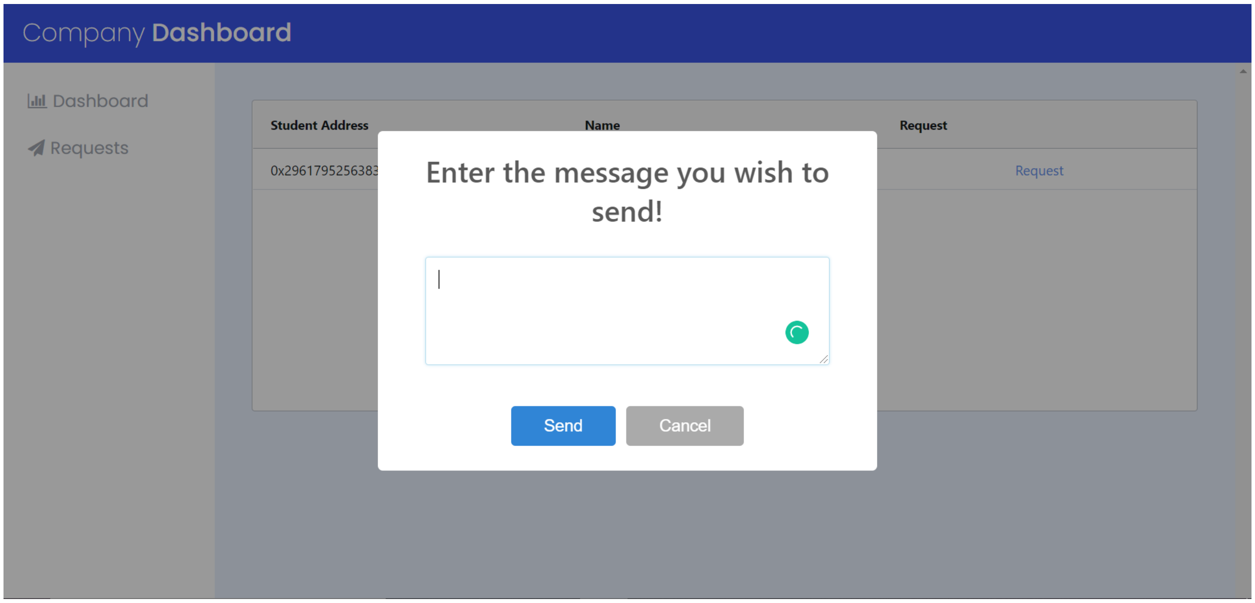
School Address	Name	View
0xb4a44441C4bd91dA50E1c06D9Cc7C79F9...	Sc1	view
0x1C9e8524874585B5931430820998Eb0E3B...	Sc2	view
0x93EC21b173d25CEd8777d8D9b2DF9bbc5...	Test School	view
0x4e686b22bF54FbB0ed1CC235bA483Df7aE...	BITS Pilani	view
0xd1AD06D70fC2396Ed3dF2322DA5DB5eCe...	BITS Pilani Demo	view

Clicking on view above you can see all the students within the school



Student Address	Name	Request
0x29617952563831c010c2FEc86A0335DE61...	Student Demo	Request

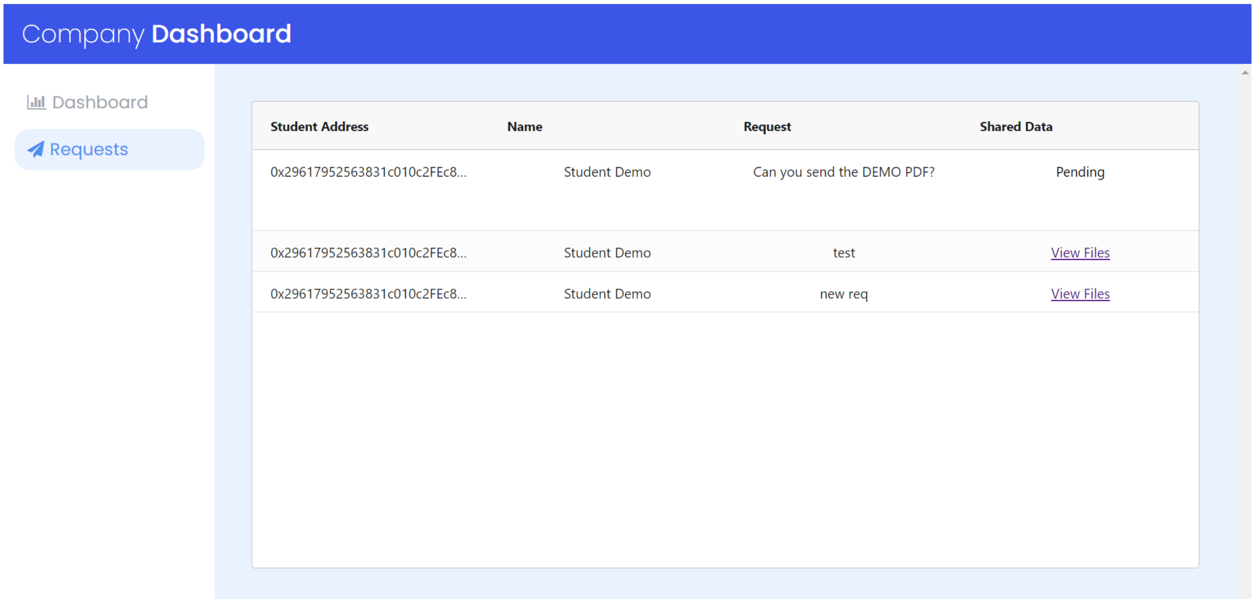
Clicking on **request** above, a modal will open where you can enter the request to the student



Student Address	Name	Request
0x2961795256383		Request

Enter the message you wish to send!

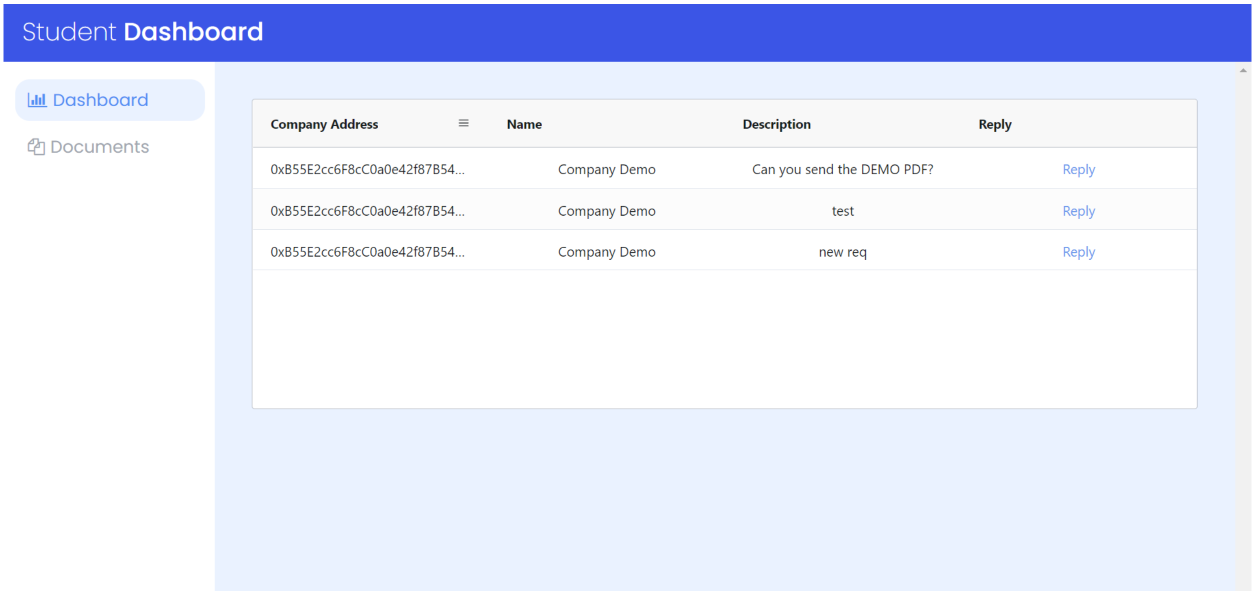
On the sidebar, if you click on requests, you can sell all the requests the company has made till now. Pending means that the student still needs to reply. Clicking on View Files, you can see the files which have been shared by the student.



Student Address	Name	Request	Shared Data
0x29617952563831c010c2FEc8...	Student Demo	Can you send the DEMO PDF?	Pending
0x29617952563831c010c2FEc8...	Student Demo	test	View Files
0x29617952563831c010c2FEc8...	Student Demo	new req	View Files

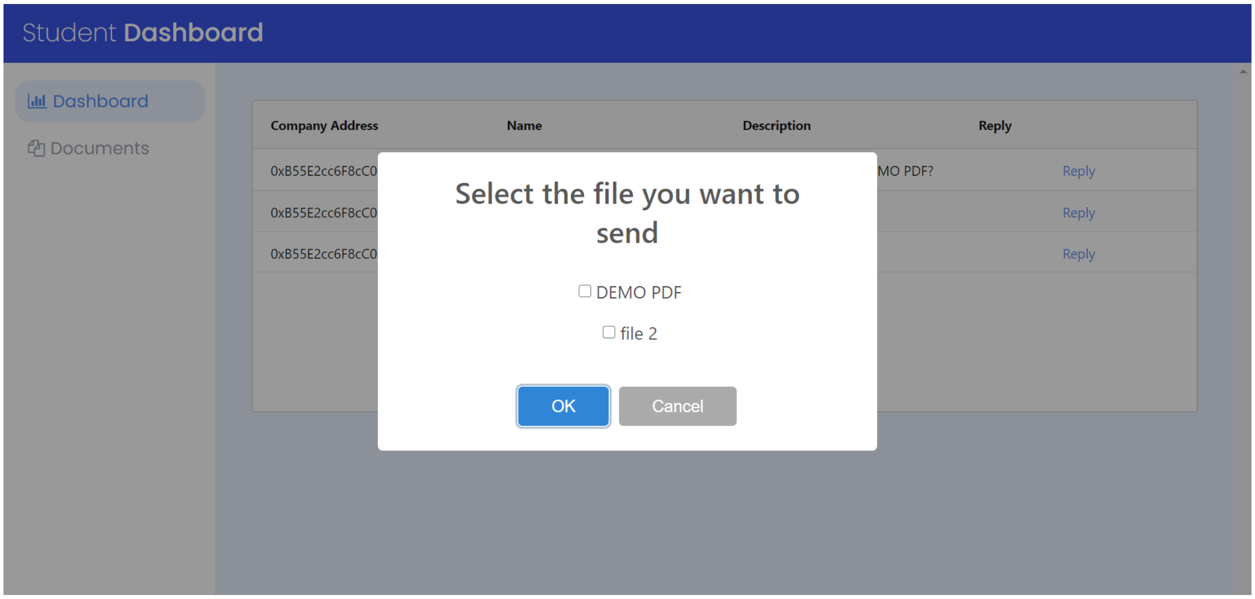
Student Dashboard

On the student dashboard you can see all the requests companies have made from the student



Company Address	Name	Description	Reply
0xB55E2cc6F8cC0a0e42f87B54...	Company Demo	Can you send the DEMO PDF?	Reply
0xB55E2cc6F8cC0a0e42f87B54...	Company Demo	test	Reply
0xB55E2cc6F8cC0a0e42f87B54...	Company Demo	new req	Reply

By replying to a request, you choose which files you wish to share

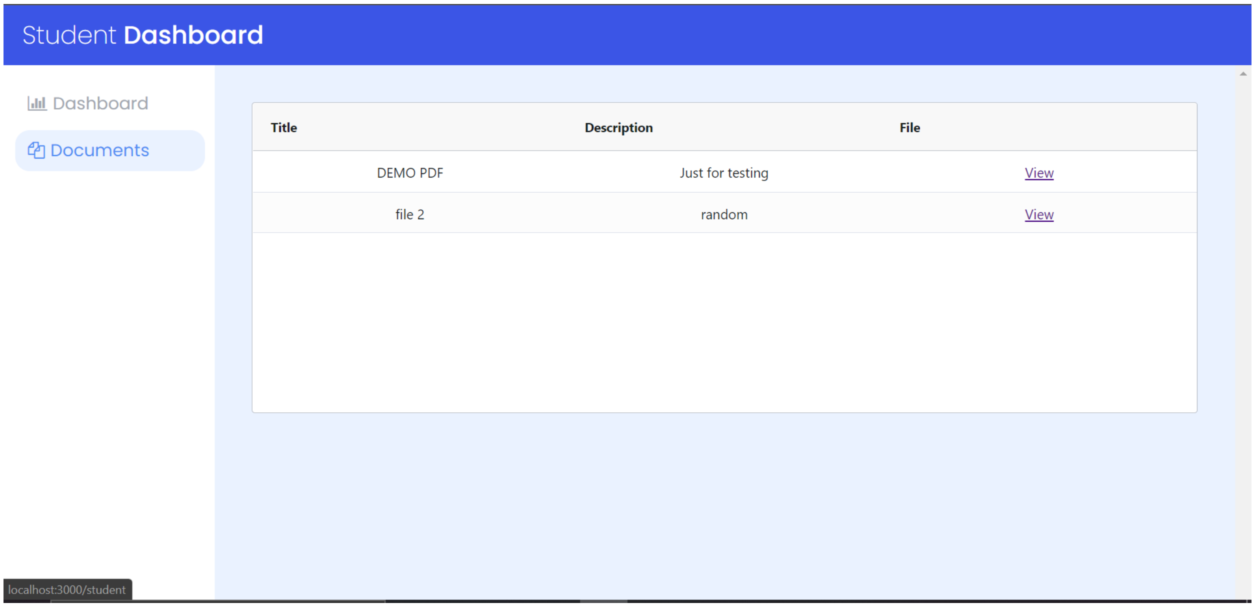


Select the file you want to send

□ DEMO PDF

□ file 2

Click on the **Documents** tab on the sidebar, the student can see what all files have been added by the Schools for the student



Title	Description	File
DEMO PDF	Just for testing	View
file 2	random	View

Advantages of Blockchain solution over traditional system:

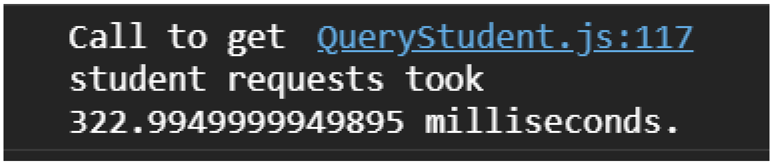
We resolved security issues revolving around the sharing of students' credentials by leveraging blockchain technology. In the traditional system, there is no security enforced by any party. When the schools hand over the documents the students have the responsibility to store them in physically secure places. Similarly, for providing documents to companies, the companies have to trust the student that they provided the correct untampered document or initiate a long verification process with the school. This is avoided due to the Smart Contract logic and the document is uploaded via a trusted entity. Moreover, the traditional system's manual work is eliminated and a properly integrated system is developed which simplifies the process for all entities. As these schools will be "writing" in the blockchain they'll spend gas and this ensures the transaction is securely completed by the miners. Students can then view their credentials and securely share it with organizations who wish to view it. Organizations can be sure that no modification has been made to the credentials and they can be trusted because of the consensus protocol.

Statistics of the project:

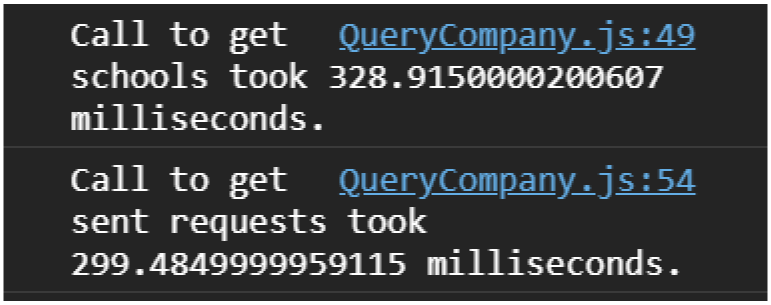
Running time and memory statistics:

For the functions that modify the blockchain:
The running time is variable and depends on the transaction being confirmed which on average takes a total of **12 seconds** for Ethereum. Although, we were accessing the Ropsten test blockchain via MetaMask so we didn't have an actual node at the blockchain but indirect access to one via MetaMask. This led to latency and on average the transaction confirmation took about **15-20 seconds** on Remix for testing environment and **30 seconds** in the actual deployed project due to other front end latencies associated.

For the functions that view the data:
All these functions are instantaneous and have complexities O(1) or O(n) where due to the small length of inputs O(n) also behaves like O(1). While testing, the time taken value for these functions came out to be close to **300ms**



```
Call to get  QueryStudent.js:117
student requests took
322.9949999949895 milliseconds.
```



```
Call to get   QueryCompany.js:49
schools took 328.9150000200607
milliseconds.

Call to get   QueryCompany.js:54
sent requests took
299.4849999959115 milliseconds.
```

Memory:
Student, School and Company addresses are stored on the blockchain which depends on the number of each.

Memory required for each user = No. of characters in the name(bytes)
+ 7 bytes(Student)
+ 6 bytes(School)
+ 7 bytes(Company)

On average = 15 bytes

Memory required for each file = 32 bytes(ipfs hash) + No. of characters in the title(bytes) + No. of characters in the description(bytes)

On average = 55 bytes

Experience from the project:

Overall from the project, we came across various limitations in the current technology and can see how it’s still in its emerging phases. However, we also had a pretty good learning experience and would like to mention them here too. We would like to thank our instructors Prof. Amit Dua and Prof. Ashutosh Bhatia for helping us learn the required concepts to implement this project and also providing us with the opportunity to practice development for Blockchain applications.

Learnings:

1. How to work in a collaborative environment
2. Exposure to decentralized app development
3. Using web3 to integrate the frontend with the smart contract code
4. Writing well structured contracts using inheritance
5. Solving gas issues and Metamask errors
6. Creating a robust frontend with proper messaged and intuitive UI

Difficulties:

1. Different behaviour of Smart Contracts in front end and back end
2. Really long redeployment process
3. Testing takes a huge amount of time and there is no other current option to do it faster
4. Manual changing of addresses hardcoded into smart contract