CIS 6930 - Blockchain: Optimization and Applications

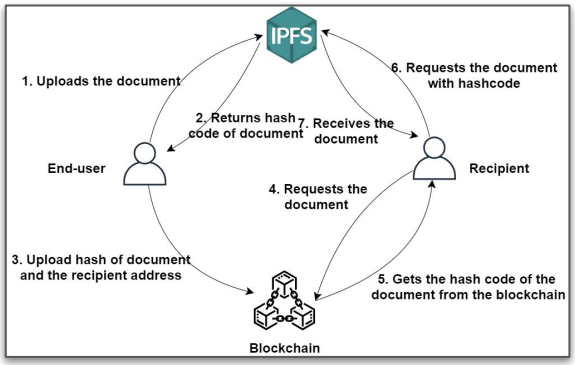
Identity ledger on Blockchain

Group 22: Ayush Sharma, Subham Agarwal, Saheel Ravindra Sawant, Rohan Sanjay Shahane

Introduction:

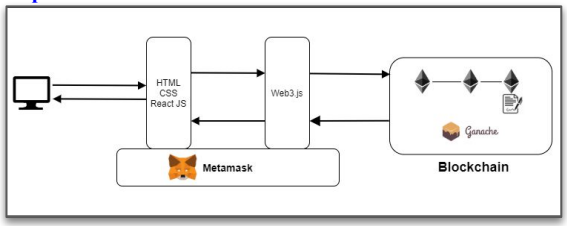
- In 2018, 2.8 billion consumer data records were exposed to cyber attackers at an estimated cost of $654 billion.
- In this project, we propose a blockchain based identity management system which gives users the ability to securely store their IDs on blockchain and provide them to designated recipient.

System Architecture:



- Storing large size of data on Blockchain is expensive. Therefore, we are storing the user's identity data on IPFS.
- The hashcode returned by IPFS is stored on the blockchain along with the respective recipient's address.
- To ensure user's data privacy, the hashcode is encrypted using recipient's public key.
- This ensures that even if an attacker procures the hash code of a file during communication, he can not access the file as the hash is encrypted.

Implementation:



- We have implemented the front-end of our application using React-JS which runs on a mobile or desktop browser.
- We used MetaMask extension to make web3 API available in our webpages. It is also used as a secure interface to review and confirm the blockchain transactions.
- The application communicates and interact with the blockchain using the Web3.js javascript library.
- We created our private Ethereum blockchain using Ganache to run tests, and also to inspect the state of our application .

Observations:

The following table shows the gas used and the transaction fee for performing the following tasks:

Task	Gas used	Cost (in ETH)
Initial Migration	196887	0.00393774
Deploy Contracts	472443	0.00944886
Share a file	270774	0.00541548
Download a file	42979	0.00085958

Conclusion:

- As of now, the application we have implemented is capable to store documents on the IPFS, encrypt its hashcode with a recipient's key and store it on the blockchain along with the address of the designated recipient for this transaction.
- We have identified a few challenges, which we will attempt to address in the rest of the semester.

Challenges:

- To keep track whether the document shared with an authorized recipient doesn't get accessed or shared with other unauthorised users who do not have access privilege.

Future scope:

- To implement a mechanism where a user who has received a document outside the application can verify the authenticity of the document and check if the sender of the document had access to this document in the first place.

References:

[1] Decentralizing privacy: Using blockchain to protect personal data, Zyskind et al., 2015 IEEE Security and Privacy Workshops.
[2] Benet, J., 2014. Ipfs-content addressed, versioned, p2p file system. arXivpreprint arXiv:1407.3561.
[3] R. A. Canessane, N. Srinivasan, A. Beuria, A. Singh and B. M. Kumar, "Decentralised Applications Using Ethereum Blockchain"
[4] Industry Brief: US Consumer Data Breach Report - https://www.forgerock.com/resources/view/92170441/industry-brief/us-consumer-data-breach-report.pdf