CS5363 Blockchain Technologies and Applications: Hw8 – Report
Decentralized App (DApp)

Name: 蘇子軒
Student Id: 106070033

Task: A DApp on Web

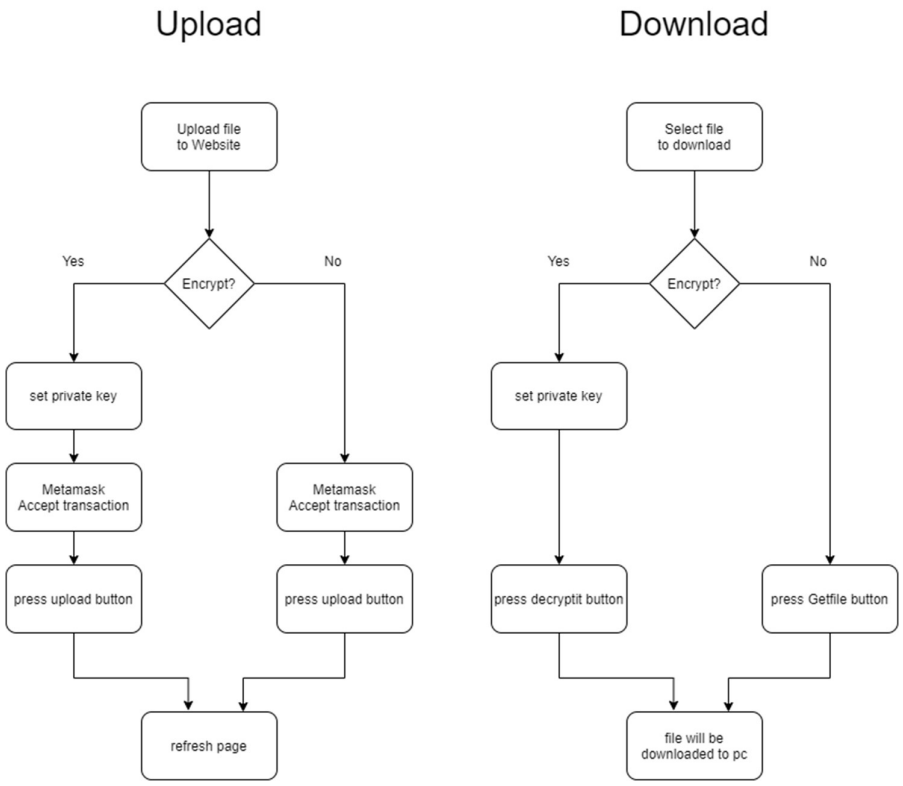
Introduction

- Product/Service Description (Describe the application scenario, including the UI & functions)

因為 IPFS 是一個免費的網路儲存空間，在網路上只要知道 hash 值便可以到 IPFS 服務的節點存取資料，因此想要有一個網站可以記錄 IPFS hash，並且附帶加密功能，使個人可以上傳並且有隱私。

Design your contracts & your web app

- Functional Description (Describe what your contracts & your web app can do)
- 上傳檔案 / 加密上傳檔 並送至 IPFS
- 下載 IPFS 檔案 / 下載 IPFS 檔案並且解密
- Design Diagram & Flow Chart (Explain the operation process in your contracts & your web app)
- User flow



- Button operation process
  - Upload files encrypt:

1. check if there is private key filled in.
2. private key turn public key.
3. generate 256 bits key.
4. encrypt file by key and use AES CTR mode.
5. encrypt key by public key.
6. send file to IPFS.
7. send file metadata and encrypted key to Ethereum.

  - Download file decrypt:

1. check if there is private key filled in.
2. get file metadata and encrypted key from Ethereum.
3. Decrypt encrypted key by private key.
4. Get file from IPFS.
5. Decrypted encrypted file and use AES CTR mode.
6. Download the decrypted result.

Test your contracts & your web app

- Test Flow Chart (Explain how can you ensure your contracts & your web app is correct)
  - Contract : use truffle test
- Test cases (Ensure your test cases provide enough testing coverage)
  - Contract:
    - Test Upload function
    - Test UploadEncrypted function
  - Website:
    - Test upload and download file type : txt, pdf, png is currently OK

Release your contracts & your web app

- Release Flow Chart (Explain how to release your contracts & your web app on the Ropsten Testnet & a public URL)
- The addresses of your contracts & their URLs on Etherscan
  0x4CF247a90956185559EE5fb2A9A7E8dDd8A8E985
- The public URL of your DApp
  https://suvincent.github.io/simpleIPFSDrive/

Other Discussion

- Any notable design concern you find…
- 目前只有 for 個人使用，因為 contract 一開始沒有想到再加開一層 mapping 區分使用者，有的話會更方便。
- File download and encryption are all in front end, not sure if there is file size limitation problem, currently the biggest file uploaded is 55KB