THE HONG KONG UNIVERSITY OF SCIENCE AND TECHNOLOGY

MSBD5017 Blockchain Final Project

Report

ZHOU, Jia Yi **20784078**

ZHU, Zhen Yi **20784183**

Chen, Zi Jie **20788256**

Email: {jzhouco, zzhubh,zchenfz}@connect.ust.hk

May 2022

Introduction

First to introduce the project background, blockchain technology has been further recognized by the government and emphasized as an infrastructure together with Big Data Technology, AI, Cloud Computing, and IoT. The Chinese mainland has banned cryptocurrency trading and mining. We believe that the development of a "coin-free blockchain" conforms to the development requirements of the digital economy era. And in many organizations (esp. government, military, and enterprises) exist a large number of confidential documents and sensitive data to be shared. And once operation errors occur (edited by mistake, deleted by mistake, malicious tamper) could cause great adverse effects. Our project mainly applies Blockchain and Distributed Storage technology on both consortium chain and private chain in the toG track. We aim to provide a safe, reliable, and traceable data-sharing platform for government, military, and other institutions with high requirements on data security.

Market

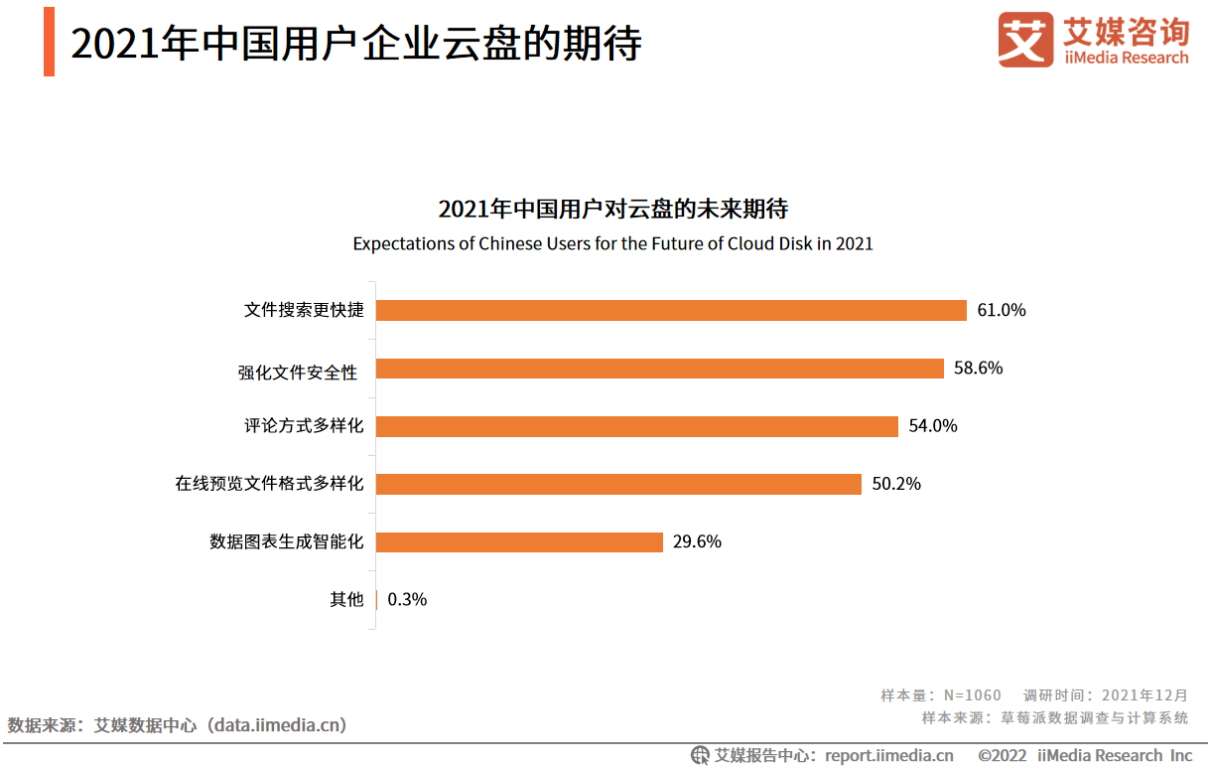

Image 1: Expectation towards Cloud disk

Outlook of current market

To the personal cloud disk: By 2021, the transaction volume of China's personal cloud market is expected to reach 2.4 billion RMB, up 42% year on year. And user's needs gradually penetrate into the direction of cross-terminal mobile office, document management collaboration, and personal digital

asset storage. And to the enterprise Cloud Disk: Amazon's cloud CEO said recently that only a small number of companies still use cloud disk services, accounting for only 4%.

Target Market

Our target markets are enterprises, governments, and the military. And they both need a secure file sharing system. The domestic regulatory principle for the cloud industry is that all Chinese data must remain in China and all technical services are expected to be provided by Chinese companies. Few of them use cloud disk services before, so the distributed file-sharing system has huge market prospects and user size in the future.

Solution

We aim to create a more reliable solution: as blockchain has security property in nature. At the same time, data on the blockchain is totally transparent. We hopes that customized permission control in such a decentralized settings can provide more flexibility comparing to the basic blockchain.
Here is the solution, the actual files and data will be stored in IPFS or other distributed file storage, and on-chain data will be the encrypted file address and other information of the file.

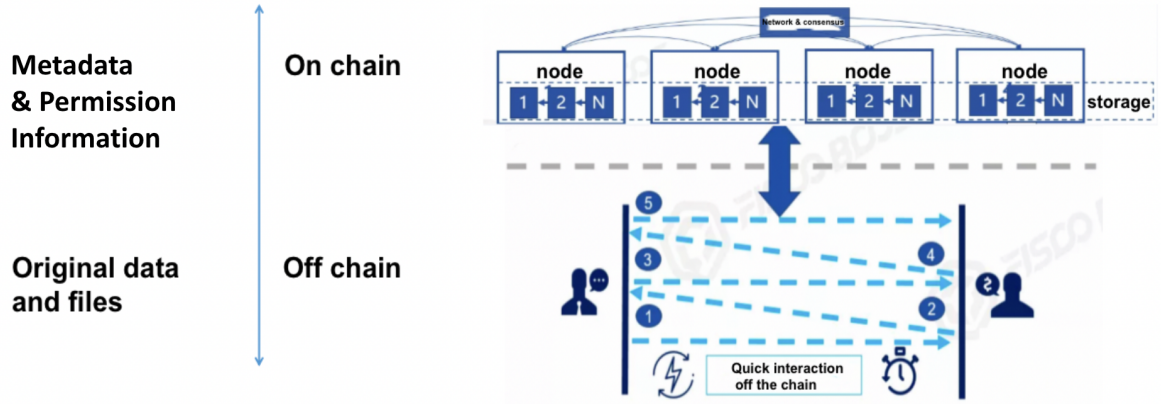

Image 2: On-chain & off-chain storage

while uploading, we store the original data in distributed file storage and upload the Metadata and transactional data to the Blockchain. While downloading, the user needs to input an encrypted file address, then the smart contract will check whether the user has permission, if the user has the right permission then the system will download the actual file from distributed file storage. The procedure was shown in the following figure.

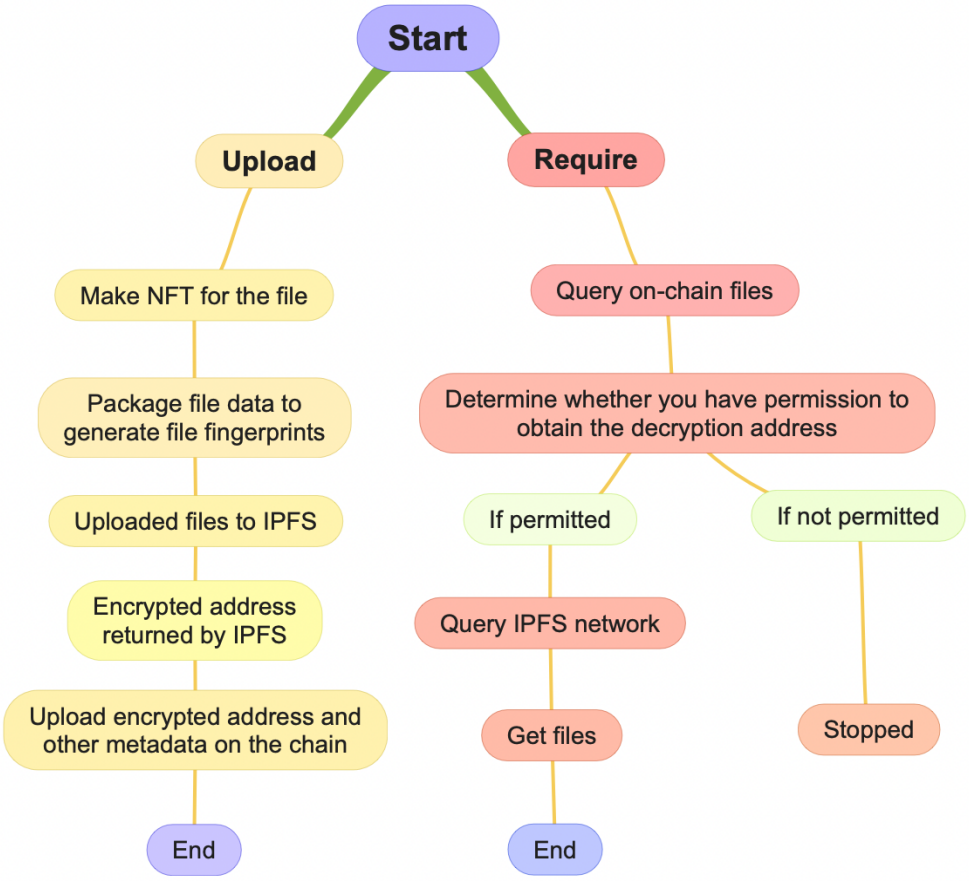

Image 3: Working flow

For now, our user interface supported function incluced:

- Upload file and assign file permission
- Download file which upload by the user
- Downlaod file which upload by other users
- Delete file which upload by the user

Here is the link for our demo:https://file-train-iota.vercel.app/

And the following is a screenshot of our demo:

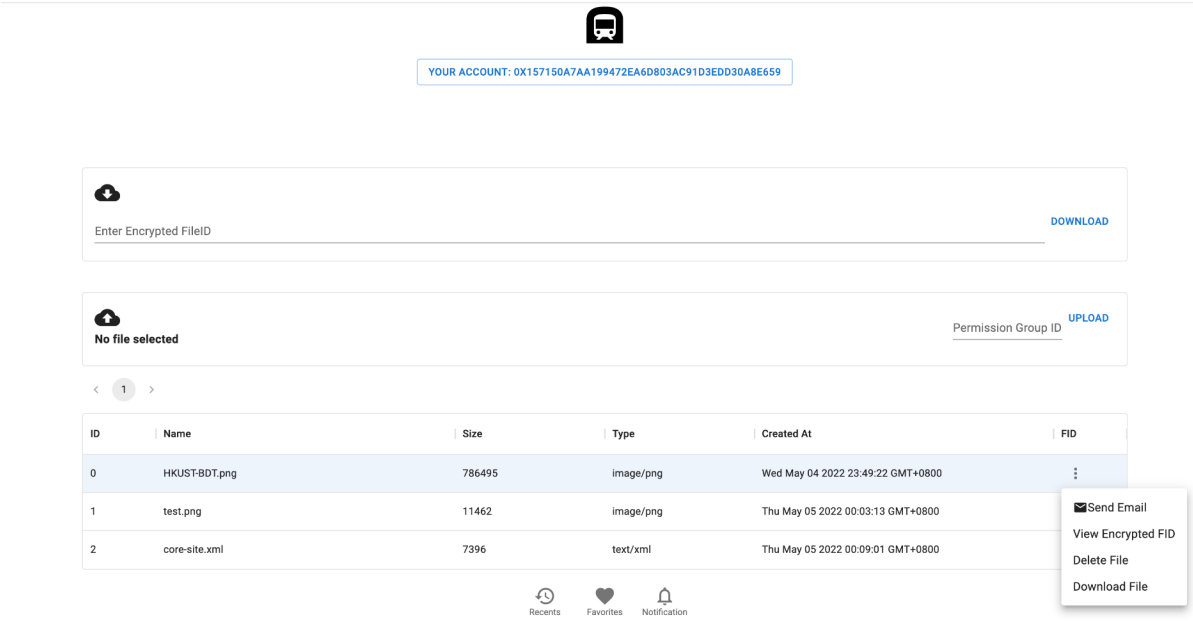

Image 4: WebUI

Block Chain

A blockchain is a distributed database that is shared among the nodes of a computer network. As a database, a blockchain stores information electronically in digital format. Blockchains are best known for their crucial role in cryptocurrency systems, such as Bitcoin, for maintaining a secure and decentralized record of transactions. The innovation with a blockchain is that it guarantees the fidelity and security of a record of data and generates trust without the need for a trusted third party. It have the following importance benefit:

- **Enhanced security**

  Your data is sensitive and crucial, and blockchain can significantly change how your critical information is viewed. By creating a record that can't be altered and is encrypted end-to-end, blockchain helps prevent fraud and unauthorized activity. Privacy issues can also be addressed on blockchain by anonymizing personal data and using permissions to prevent access. Information is stored across a network of computers rather than a single server, making it difficult for hackers to view data.
- **Greater transparency**

  Without blockchain, each organization has to keep a separate database. Because blockchain uses a distributed ledger, transactions and data are recorded identically in multiple locations. All network participants with permission access see the same information at the same time, providing full transparency. All transactions are immutably recorded, and are time- and date-stamped. This enables members to view the entire history of a transaction and virtually eliminates any opportunity for fraud.
- **Instant traceability**

Blockchain creates an audit trail that documents the provenance of an asset at every step on its journey. In industries where consumers are concerned about environmental or human rights issues surrounding a product — or an industry troubled by counterfeiting and fraud — this helps provide the proof. With blockchain, it is possible to share data about provenance directly with customers. Traceability data can also expose weaknesses in any supply chain — where goods might sit on a loading dock awaiting transit.

- **Increased efficiency and speed**
  Traditional paper-heavy processes are time-consuming, prone to human error, and often require third-party mediation. By streamlining these processes with blockchain, transactions can be completed faster and more efficiently. Documentation can be stored on the blockchain along with transaction details, eliminating the need to exchange paper. There's no need to reconcile multiple ledgers, so clearing and settlement can be much faster.

Automation

Transactions can even be automated with "smart contracts," which increase your efficiency and speed the process even further. Once pre-specified conditions are met, the next step in the transaction or process is automatically triggered. Smart contracts reduce human intervention as well as reliance on third parties to verify that the terms of a contract have been met. In insurance, for example, once a customer has provided all necessary documentation to file a claim, the claim can automatically be settled and paid.

Solidity

Solidity is an object-oriented, high-level language for implementing smart contracts. Smart contracts are programs that govern the behavior of accounts within the Ethereum state. Solidity is used to support our app to communicate with the chain. Seveal function have implemented addfile, deleteFile, check_permission and getFilesInRange for displaying files.

IPFS

IPFS is a distributed system for storing and accessing files, websites, applications, and data. It is a peer-to-peer (p2p) storage network. Content is accessible through peers located anywhere in the world, who might relay information, store it, or do both. IPFS knows how to find what you ask for using its content address rather than its location. Only people who know the file address can access the files. Also, such kind of file storage effectively reduces data redundancy by generating same file id for different files with the same content.

Future Plan

We have two future plans, the first is the technology track plan. We would like to expand to federal learning with privacy computing.

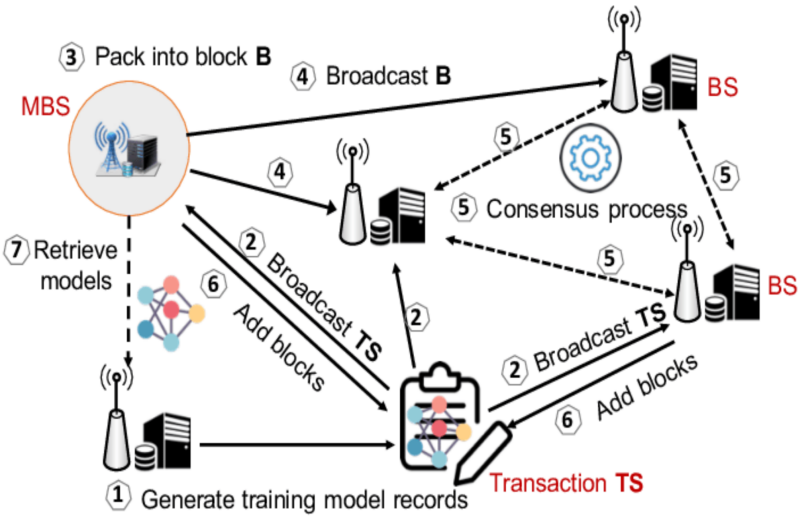

Image 5: Federal Learning with privacy

and enable the secure computation of the data without revealing the content of the data the following is the sketch map.

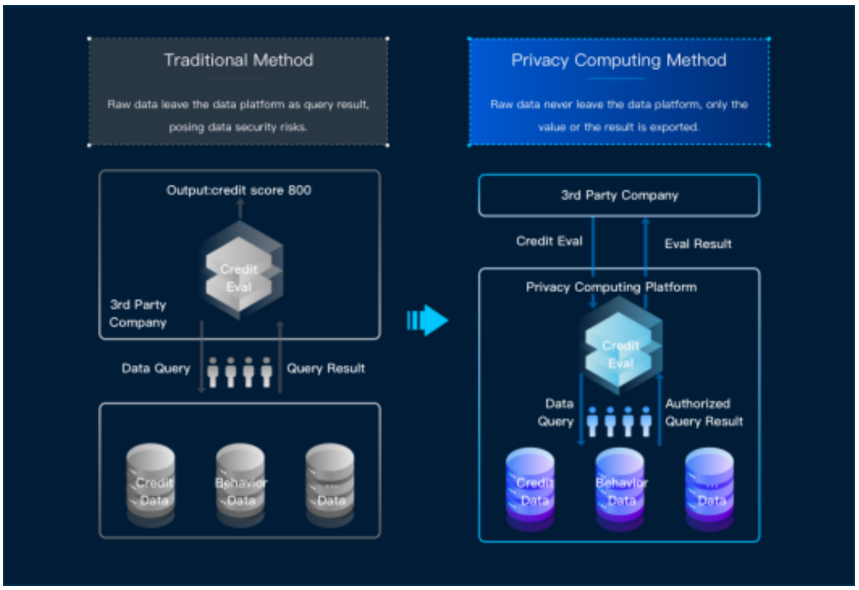

Image 6: Privacy computing Method

And our Business Track Plan is we would write our whitepaper and set up our business roadmap, and then establish the association, to our Chinese market we will connect with government, enterprises and military and to our overseas market, we would like to use some communication tools such as

Discord, Telegram to attract people to join our ecosystem; And then hire Twitter influencer to promote; And then Convince cryptocurrency kingpins to invest and use.

Contribution

ZHOU Jiayi:

- Responsible for the initial idea
- Technical architecture which includes designing working flow and technology selection
- Command-line app development including deploying the IPFS cluster (which is not included in the final version)
- Web app development
- Smart contract development
- Presentation slides
- Report

Chen Zijie:

- Web app development
- Optimizing working flow
- Smart contract development
- Presentation slides
- Report

Zhu Zhenyi:

- Web app development
- Optimizing working flow
- Smart contract development
- Presentation slides
- Market analysis and business plan
- Report

Reference

ETD https://sdk.docs.etdchain.net/docs/intro
IPFS https://docs.ipfs.io/
Hardhat https://hardhat.org/getting-started/#quick-start
Smart contract https://ethereum.org/en/developers/docs/ethereum-stack/
Next.js https://nextjs.org/docs
Market analysis https://www.iimedia.cn/c1020/83440.html