# IPFS 文件管理与共享平台的设计与实现

## 一、立题依据

### 1.研究的目的与意义

可信文件存储是目前互联网系统中的一种新型架构，传统的文件存储不能保证文件存储可信。当企业用户向企业发起存储文件请求时，企业会将企业用户的文件存储在服务器上，当企业用户需要时，再从服务器上将文件取出返回。由于文件仅仅存储在一个企业的服务器上，一方面不能保证文件的可信，文件有可能会被修改；另一方面，一旦企业的服务器不可用，用户便无法再获取文件。

而 IPFS 网络是完全去中心化的，网络中的节点互相提供文件，且通过文件 hash 确保文件的完整性。IPFS 是基于内容的寻址，不是基于位置的寻址。IPFS 通过 CID 实现内容寻址，CID 即内容标识符，是用来指向 IPFS 中文件的标签。CID 是基于内容的加密hash，内容上的任何差异都会产生不同的 CID，使用相同的设置添加到两个不同 IPFS 节点的相同内容将生成完全一样的 CID。当下载文件时，IPFS 网络上的主机若存储有相同 CID 的文件，便会提供文件。下载文件之后，CID 会被用来校验文件是否被篡改。IPFS 使用内容寻址的另一个好处是去除重复文件，当多个人在IPFS上发布同一文件时，该文件只会创建一次，这会使网络非常高效地运行。

目前 IPFS 有以下几点不足：

1）目前用户可以通过 IFPS 客户端上传文件，上传的文件记录会保存在本地的数据库中，但若不小心将该数据库文件删除或系统宕机，用户的上传文件记录就会丢失。

2）IPFS 存在用户之间共享文件繁琐的问题，若用户想要将文件分享给其他用户，需要复制文件的 CID 给每一个人。

3）IPFS 中的文件公开存储，若文件的 CID 泄露，任何人都能下载此文件。

4）若文件已经上传到 IPFS 中，但是由于没有主机持有该文件或者持有该文件的主机连接较差，该文件的下载服务就暂时不可用。

因此，本课题计划设计并实现 IPFS 文件管理与共享平台。IPFS 文件管理系统为用户提供管理 IPFS 中文件的功能，一方面便于用户方便地在网页端将 IPFS 中的文件归类整理，另一方面即使用户本地的文件记录丢失，用户也能从平台中找回自己的文件记录。IPFS 文件共享系统主要包括群组功能和资源发布功能，通过建立群组，实现群组内资源共享，而将资源发布可以让系统内所有用户都能查看并下载文件资源。

### 2.研究现状和发展趋势

由 Fluence Labs 发布的《去中心化开发人员 2020》报告的结果表明， IPFS 和以太坊是迄今为止用于创建 DWeb 应用程序的领导者。

IPFS 全称 InterPlanetary File System，是一个旨在创建持久且分布式存储和共享文件的网络传输协议。IPFS是一种内容可寻址的对等超媒体分发协议。在 IPFS 网络中的节点将构成一个分布式文件系统。 IPFS 是点对点的超媒体协议，可以让网络更快、更安全、更开放。数据在 IPFS 上的存储都是以碎片的形式存储的，每个碎片的大小是 256k。网络中的节点会对文件的碎片进行存储。当检索数据时，所有文件的碎片会被收集起来，通过文件管理系统按序组合碎片得到想要下载的文件。整个 IPFS 网络中没有中心服务器，是完全去中心化的。

Filecoin 是运行在 IPFS 上面的一个激励层。分布文件的行为，完全是自愿的，为了让 IPFS 协议能够被更多人使用，让更多的人愿意拿出自己的电脑和存储空间给其他人使用，Protocol Labs 公司创建了 Filecoin 这个项目。Filecoin 是一个去中心化存储网络，它让云存储变成一个算法市场。这个市场运行在有着本地协议令牌（也叫做 Filecoin）的区块链。区块链中的矿工可以通过为客户提供存储来获取 Filecoin。

除了使用 IPFS 协议的 Filecoin，还有不少其他用于分布式存储的加密货币。其中知名度比较高的有 Sia、Storj、Swarm 和 Lambda：

(1) Sia: Sia[4] 在数据切分过程中采用 Reed-Solomon 编码 [5] ， 来提高数据的可恢复性。Sia 交易匹配方式是存储提供方设定价格，存储需求方进行挑选，然后提交匹配订单。但是目前 Sia 采用 POW 共识机制来对交易进行验证，无法适用于高频实时结算的场景。

(2) Storj: Storj 是一个云存储项目 [8] ，本质上和区块链没有关系，只是在结算时采用了以太坊的 ERC-20 Token。Storj 基于“即用即付”的设计方式，用户自定义一对一存储、还是一对多存储。但是用户需要保持长时间的在线，来确保存储设备是否正常工作，用户体验较差，而且 Storj 基于以太坊进行交易结算，很明显也无法应用于高频的交易场景。

(3) Swarm: 另一个在以太坊网络上的分布式存储协议，名为 Swarm，基本上和 Filecoin 的技术差不多，但是发展要比 IPFS 慢一些。

(4) Lambda: Lambda 是一个中国团队项目，获得了多家投资机构站台。作为一个分布式存储的项目，它解决的问题是在分布式存储中，用户把自己的文件交由未知的存储端时产生的信任的问题，而 Lambda 通过验证节点的共识完成文件数据的持有性证明和可恢复性证明，保证了存储在未知存储端上文件的完整性和可恢复性。

## 二、研究内容和目标

### 1.课题研究内容

本课题计划在 IPFS 去中心化的基础上，为用户提供线上的用户文件管理与用户间的文件资源共享与交流平台。

### 2.研究目标与效果

（1）为用户提供管理在 IPFS 上存储的文件的功能

1）用户上传文件

用户可以上传本地的文件到系统中，由系统上传到 IPFS 中。

若文件之前已经被上传到 IPFS 中，用户可以直接输入文件对应的 cid。

如果用户想要上传某链接里的文件，可以直接填写文件链接，系统会在下载对应链接里的文件之后，将文件上传到 IPFS 中。

2）用户文件管理

用户可以创建文件夹，也可以移动文件或文件夹到其他文件夹。

此外，用户可以删除文件或文件夹。

3）查看文件

系统检测文件的格式，为用户提供查看文件的功能，包括阅读文本，播放音频文件，播放视频文件。

4）文件（夹）分享

用户可以分享文件或文件夹，并设置分享的有效时间，系统会为用户生成分享链接和相应的密码。用户可以将链接和密码分享给其他用户。

如果过了有效时间，分享链接会失效，其他用户就无法访问相应的文件。

通过这种方式分享资源，可以避免资源的 CID 被泄露。

（2）群组功能

1）组长创建群组，邀请组员加入群组，组长可以编辑群组内的共享资源。

2）组员可以查看群组内的文件资源，或者将文件资源加入自己私人的文件列表中，但是没有编辑权限。

3）群组内有交流板块，组员之间可以互相交流

（3）IPFS 资源共享交流平台

1）发布资源

用户发布的资源是一系列文件与文件夹的集合。用户可以在平台上发布资源，并为资源添加资源名称与相关描述信息。发布的资源在平台上是共享的，所有用户都可以浏览或下载自己感兴趣的资源。

2）资源讨论区

每个资源下面都有一个讨论区，用户可以在讨论区里进行讨论和交流。

3）资源搜索

用户可以搜索资源，输入关键词，系统将列出包含关键词的所有资源。

4）资源排序

资源默认按照发布时间排列，也可以按照下载量和评论数进行排序。

5）热门资源展示板块

系统统计并展示最近 1 个月的热门资源

### 3.拟解决的关键问题