IPFS技术详解1

1.IPFS介绍

1.1 IPFS简介

IPFS，星际文件系统(InterPlanetary File System) / 超媒体协议，它本质上是一种内容可寻址、版本化、点对点超媒体的分布式存储、传输协议，其目标是补充甚至取代过去20年里使用的超文本媒体传输协议（HTTP） 。基于通信网络的发展，未来下载速度会远大于硬盘读写速度，它的期望是把全世界连接成一块大硬盘，终端设备不需要存储太多数据，大部分数据从云端下载，从而构建更快、更安全、更自由的互联网时代。

- IPFS是一个协议
- IPFS是一个文件系统
- IPFS是一个web
- IPFS是模块化的协议
- IPFS是一个p2p系统
- IPFS是一个CDN

1.2 HTTP的不足

- 低效，成本高
- 数据删除频繁
- 主干网依赖严重
- DDOS攻击泛滥
- 作为人类文明的平衡器和创新加速器，这种作用正在日益受到威胁

1.3 IPFS VS HTTP

IPFS弥补了HTTP的不足，带来了以下改变：

- 文件存储的方式改变

  基于内容寻址，而非域名寻址，文件（内容加密的哈希值）具有存在的唯一性，大大地减少了存储系统的数据冗余。

- 数据在互联网上传输的方式

- 人类使用数据的方式

IPFS的网络上运行着一条区块链，即用来存储互联网文件的哈希值表，每次有网络访问，即要在链上查询该内容（文件）的地址。

- 存储资源的优化配置
- 带宽资源的优化配置

1.4 互联网服务模式的迭代历程

- 集中化模式

  不足：服务高度依赖中心网络，带宽成本高

- 分散集群模式

  不足：数据有丢失风险，带宽成本高

- 去中心化分布式集群模式

  IPFS：给定的哈希指纹和路径名，要做的事情是启动一个本地节点，对该网关发一个寻址PIN的请求，IPFS自动索引分布式哈希表的哈希值，找到指纹b所对应的节点列表。

  大文件通常不会都存在一个节点，可能分片存在其它一些子节点上，IPFS把这些节点列表全部并行抓取，最后由本地的manager拼成完整的文件。并行的速度远远大于直接下载完整文件的速度，很快就能在本地取得完整文件，还可以继续分享给其他人。

2.IPFS架构

2.1IPFS协议栈

IPFS有八层协议栈，从上至下为身份、网络、路由、交换、对象、文件、命名、应用，每个协议栈各司其职，又互相搭配。

通过这八层协议栈，提高了效率，降低了系统的成本。

- 身份层和路由层。对等节点身份信息的生成以及路由规则是通过Kademlia协议生成制定，KAD协议实质是构建了一个分布式松散Hash表，简称DHT，每个加入这个DHT网络的人都要生成自己的身份信息，然后才能通过这个身份信息去负责存储这个网络里的资源信息和其他成员的联系信息。如同微信名片分享，在无法通过直接搜索微信号的情况下，如果你要找一个人，可以通过有这个人联系方式的朋友分享名片来建立联系。

- 网络层。使用的LibP2P可以支持任意传输层协议。NAT技术提供内网穿透功能。

- 交换层。是类似迅雷这样的BT工具。迅雷其实是模拟了P2P网络，并创建中心服务器，当服务器登记用户请求资源时，让请求同样资源的用户形成一个小集群swarm，在这里分享数据。这种方式有弊端，一位服务器是由迅雷统一维护，如果出现了故障、宕机时，下载操作无法进行。

  中心化服务还可以限制一些下载请求，人们发明了一种更聪明的方式就是Bittorrent，让每一个种子节点所要存储的数据，通过哈希表存储在里面，BT工具相对不太受监管，服务更加稳定。

  IPFS团队把BitTorrent进行了创新，叫作Bitswap，它增加了信用和帐单体系来激励节点去分享，我推断FileCoin有很大概率是基于Bitswap，用户在Bitswap里增加数据会增加信用分，分享得越多信用分越高。如果用户只去检索数据而不存数据，信用分会越来越低，其它节点会在嵌入连接时优先选择信用分高的。

  这一设计可以解决女巫攻击，信用分不可能靠机器刷去提高，一直刷检索请求，信用分越刷越低。请求次数和存储量的变量之间有一个比较精妙的算法，类似一个抛物线，前期可以容忍很多东西，达到一定次数后不再信任。

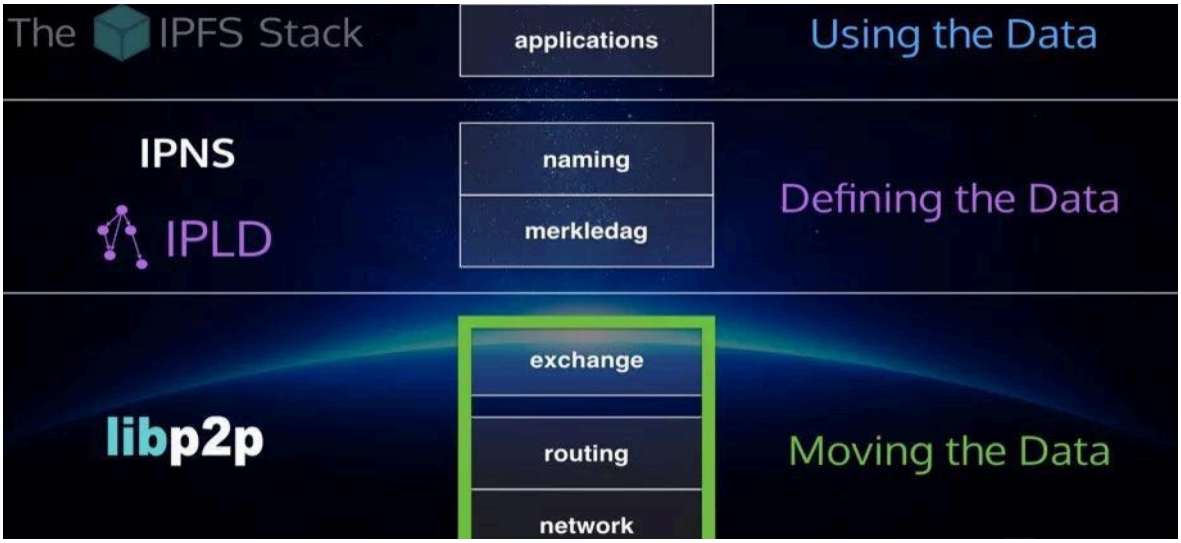
- 对象层和文件层。它们管理的是IPFS上80%的数据结构，大部分数据对象都是以MerkleDag的结构存在，这为内容寻址和去重提供了便利。文件层是一个新的数据结构，和DAG并列，采用Git一样的数据结构来支持版本快照。

- 命名层。具有自我验证的特性（当其他用户获取该对象时，使用指纹公钥进行验签，即验证所用的公钥

是否与NodeId匹配，这验证了用户发布对象的真实性，同时也获取到了可变状态），并且加入了IPNS这个巧妙的设计来使得加密后的DAG对象名可定义，增强可阅读性。

- 应用层。IPFS核心价值就在于上面运行的应用程序，我们可以利用它类似CDN的功能，在成本很低的带宽下，去获得想要的数据，从而提升整个应用程序的效率。

2.2 IPFS技术结构



- DHT:分布式哈希表
- BitTorrent:BT协议

  IPFS和BT/迅雷没有本质区别

- Git: 版本化

  提供文件的历史版本控制器，并且让多节点使用保存不同版本的文件

- SFS：自认证命名

2.3 IPFS族谱关系

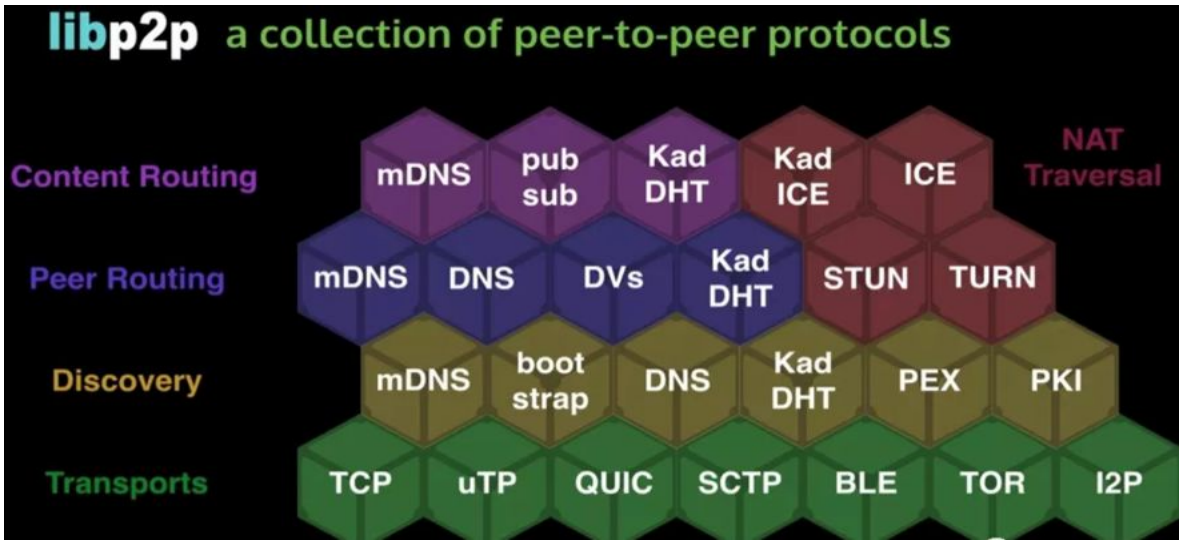
- 开发者：协议实验室（https://protocol.ai/projects/）
- 主页目前有5个核心项目，其关系如下：

2.4 Libp2p介绍

IPFS团队将点对点(peer-to-peer)网络的网络层从IPFS工程里面分离出来，形成一个独立的项目，这就是libp2p。该项目不仅可以供IPFS使用，也可以提供其它项目使用，作为一个p2p工程的底层协议存在。

主要功能：

- 发现节点
- 连接节点
- 发现数据
- 传输数据



2.5 IPLD介绍

PLD定义了基于内容寻址的统一数据结构类型。它是一个转换器，可以把现有的异构的数据结构（基于内容寻址）统一成一种格式，方便不同系统之间的数据交换和互操作。

通过哈希进行内容寻址的技术已经广泛应用于各种分布式系统。从加密货币的区块链到备份代码的每一次提交，再到各种web内容，他们背后的逻辑几乎是相同的，然后由于数据结构的不兼容，造成了这些数据无法互相操作。IPLD作为中间层统一了这些异构的数据结构，使得不同的数据可以进行数据交换。

IPLD的组成：

```
CID（Self-describingcontent-addressed identifiers for distributed       systems）：
基于内容寻址的自我描述标识

IPLDtree：基于 JSON、Protobuf和路径导航的跨协议的数据模型

IPLD Resolvers：IPLD转换器，可以添加新的协议到IPLD里面

Multiformats

Multiformats是一系列协议的集合，它在现有协议基础上对值（值：通常是具有某一项表达意义的）进行自我描述改造，即从值上就可以知道该值是如何产生的。

当前multiformats协议里面包含以下协议。

        multihash- self-describing hashes

        multiaddr- self-describing network addresses

        multibase- self-describing base encodings

        multicodec - self-describingserialization

        multistream- self-describing stream network protocols

        multigram(WIP) - self-describing packet network protocols
```

通常情况下我们使用的哈希计算方法都是某一种实现方式，比如sha1，sha2-256等。哈希计算在软件工程里面几乎随处可见，特别是区块链项，multiformats将所有的哈希值计算统一成同样的格式，为系统开发带来很多好处

以multihash为例：

升级后的哈希值的结构为：

<哈希函数类型><摘要长度><摘要值>

有一个使用sha2-256函数生成的哈希值（如下），其长度为32（16进制0x20）：

41dd7b6443542e75701aa98a0c235951a28a0d851b11564d20022ab11d2589a8

规定sha2-256的代表数字为12(16进制)，于是得出来新的哈希值：

122041dd7b6443542e75701aa98a0c235951a28a0d851b11564d20022ab11d2589a8

新的哈希值具有自我描述性质，它说明了自己是怎么来的

2.6 Filecoin介绍

IPFS只是一个协议, 并不是挖矿软件本身。Filecoin系统才是挖矿软件本身, 代币名字是 FIL。Filecoin使用了IPFS 协议来运行系统。

2.6.1 Filecoin总结

- Filecoin是一个区块链项目，建立在IPFS之上，是IPFS的积累层
- Filecoin采用了创新的共识机制：PoSt（时空证明，一定的时间一定的空间一定的数据）
- Filecoin采用硬盘挖矿，共享硬盘

  需要解决的难点：如何保证矿工不作弊，即下载所有的数据后验证是不合理的。

  矿工的影响力：存储的数据占全网的比例

2.6.2 Filecoin代币：FIL

```
FIL代币总共有20亿枚。分配方案，总共有四个部分组成：

70%作为挖矿的回报：像比特币一样根据挖矿的进度逐步分发

15%预留Protocol Labs：作为研发费用，6年逐步解禁

10%分配给ICO投资者： 根据挖矿进度，逐步解禁

5%预留给Filecoin基金会： 作为长期社区建设，网络管理等费用， 6年逐步解禁

私募时间：2017.07.21-2017.7.24

成本：0.75美元

行权期：1-3年，折扣额0-30%

参与人数：150+人

募集金额：0.52亿美元

公募时间：2017.08.07-2017.09.07

成本：1-5美元

行权期：1-3年，折扣额0-30%

参与人数：2100+人

募集资金：2.05亿美元
```

2.6.3 Filecoin交易市场

- Filecoin存储市场(Filecoin Storage Market)-存储矿工

  链上交易，系统匹配订单，双方签名数据上链。

  数据存储市场所需要贡献的就是硬盘存储空间，越多的硬盘空间，挖矿能力就越高，存储市场采用的工作量证明是PoS(Power of Storage)证明，根据存储的数据大小来按比例分配FIL。

- Filecoin数据检索市场(Filecoin's Retrieval Market)-检索矿工

  即下载数据，链下交易，提高性能。先交易，交易完成后双方签名写入链。

  检索矿工转发数据需求，留言协议。

  数据由存储矿工定价。

  数据检索市场贡献带宽，根据访问数据的流量来分配FIL。

2.6.4 Filecoin场景

- 用户场景：

  a.用户提交数据存储订单（PUT）给Filecoin系统

  b.用户提价数据检索订单（GET）给Filecoin系统

  c.如果上述订单达成，用户支付FIL以获取相应的服务

- 存储矿工场景：

  a.在区块链上注册自己硬盘空间，注册完成后硬盘空间将被记录到区块链的配置表里面

  b.接受订单，用户提交的存储订单（PUT）

  c.订单交易达成后，双方对交易进行签名，矿工完成数据存储，交易完成后该交易被记录到区块

  d.用户获取到对应的支付

- 检索矿工场景：

  a.接受订单，用户提交数据查询订单（GET）

  b.交易达成后，双方对交易进行签名，矿工把数据发送给用户，该交易提交到区块

2.6.5 Filecoin证明

- 数据持有性证明（Provable Data Possession ，PDP)：用户发送数据给矿工进行存储，矿工证明数据已经被自己存储，用户可以重复检查矿工是否还在存储自己的数据
- 可检索证明（Proof-of-Retrievability，PoRet）：和PDP过程比较类似，证明矿工存储的数据是可以用来查询的
- 存储证明（Proof-of-Storage ，PoS）：利用存储空间进行的证明。工作量证明的一种，Filecoin上一篇论文使用了这个名字，新的论文则升级为PoRep
- 复制证明（Proof-of-Replication，PoRep）：新的 PoS（Proof-of-Storage），PoRep可以保证每份数据的存储都是独立的，可以防止女巫攻击，外源攻击和生成攻击
- 工作量证明（Proof-of-Work，PoW）：证明者向检验者证明自己花费了一定的资源，PoW被用在加密货币，拜占庭共识和其他各种区块链系统。BTC使用的就是这种类型的证明，依赖巨量的哈希计算和能源消耗来建立共识和保证btc网络的安全性
- 空间证明（Proof-of-Space，PoSpace）：Filecoin提出的概念，存储量的证明，PoSpace是PoW的一种，不同的是PoW使用的计算资源，而PoSpace使用的是存储资源
- 时空证明（Proof-of-Spacetime，PoSt)：时空证明，矿工证明自己花费了spacetime资源,即：一定时间

内的存储空间的使用，PoSt是基于PoReps实现的

3.IPFS应用意义

- 可以为内容创作带来一定的自由。

  代表应用：Akasha

  Akasha（ https://blog.akasha.world ）是一个基于以太坊和IPFS的社交博客创作平台，用户创作的博客内容通过一个IPFS网络进行发布，而非中心服务器。

  同时，用户和以太坊钱包账户进行绑定，用户可以对优质内容进行ETH打赏，内容创作者能以此赚取ETH，如同人脑挖矿一样。它没有太多监管的限制，也没有中间商抽成，内容收益直接归创作者所有。

- 可以降低存储和带宽成本。

  代表应用：Dtube

  Dtube（https://d.tube）是一个搭建在Steemit上的去中心化视频播放平台，其用户上传的视频文件都经过IPFS协议进行存储，具有唯一标识。相较于传统视频网站，它降低了同资源冗余程度，同时大大节约了海量用户在播放视频时所产生的带宽成本。

- 可以与区块链完美结合。

  代表应用：EOS

  运用IPFS技术解决存储瓶颈是目前来看的过渡方案，最典型的应用就是EOS。EOS引以为傲的是可以支持百万级别TPS的并发量，其中除了DPOS共识机制的功劳之外，还归功于其底层存储设计是采取IPFS来解决大型数据的传输效率。

  EOS将自己打包好的区块数据通过IPLD进行异构处理，统一成一种便于内容寻址的数据结构类型，并挂载到IPFS的link上，让IPFS网络承担存储和P2P检索的逻辑，而不消耗EOS区块链系统本身太多的计算资源。

- 可以为传统应用提供分布式缓存方案。

参考：

```
1.[http://www.8btc.com/ipfs-application](戴嘉乐：详解IPFS的本质、技术架构以及应用.)

2. [https://blog.csdn.net/a791693310/article/details/80612676](IPFS学习笔记.)
```

推荐：

```
1.[http://ipfser.org](IPFS社区)
2.[https://protocol.ai/projects/](协议实验室主页)
3.[《IPFS指南》](董天一.IPFS/Filecoin中国区技术布道人)
```