

IPFS简介及如何在BSN中使用IPFS



目录

Contents



什么是IPFS?



为什么需要
IPFS?



IPFS架构及特
性



Filecoin



如何在BSN中使
用IPFS

什么是HTTP?

HTTP（超文本传输协议HyperText Transfer Protocol, Http）用于在Internet上发送和接收消息。是以超文本传输为目的而设计的应用层协议，基于TCP/IP实现的协议。此协议传送的数据形式可以是普通正文、超文本、音频、视频等等。

用户使用http://或https://链接指向网页、图像、电子表格、数据集或者推文等时，用户按其位置识别内容，这是位置寻址。该链接是指向web上的特定位置的标识符，其对应于web上某处的特定服务器或服务器组，控制该位置的人控制内容。



什么是IPFS?

IPFS (InterPlanetary File System, 中文名叫星际文件系统) 是一个基于内容寻址的、分布式的、新型超媒体传输协议。原理用基于内容的地址替代基于域名的地址, 也就是用户寻找的不是某个地址而是储存在某个地方的内容, 它旨在使网络更快、更安全、更开放。

<http://kb.bsnbase.com/actionImg/PubPlayMedia.do?id=2c908ad371c6396b01752f320f5c5a1a>

<https://ipfs.io/ipfs/QmQK6V4WScFyhXduqdjT1BSDwbj1NHQc8ToKa8ERmFU4Wk>



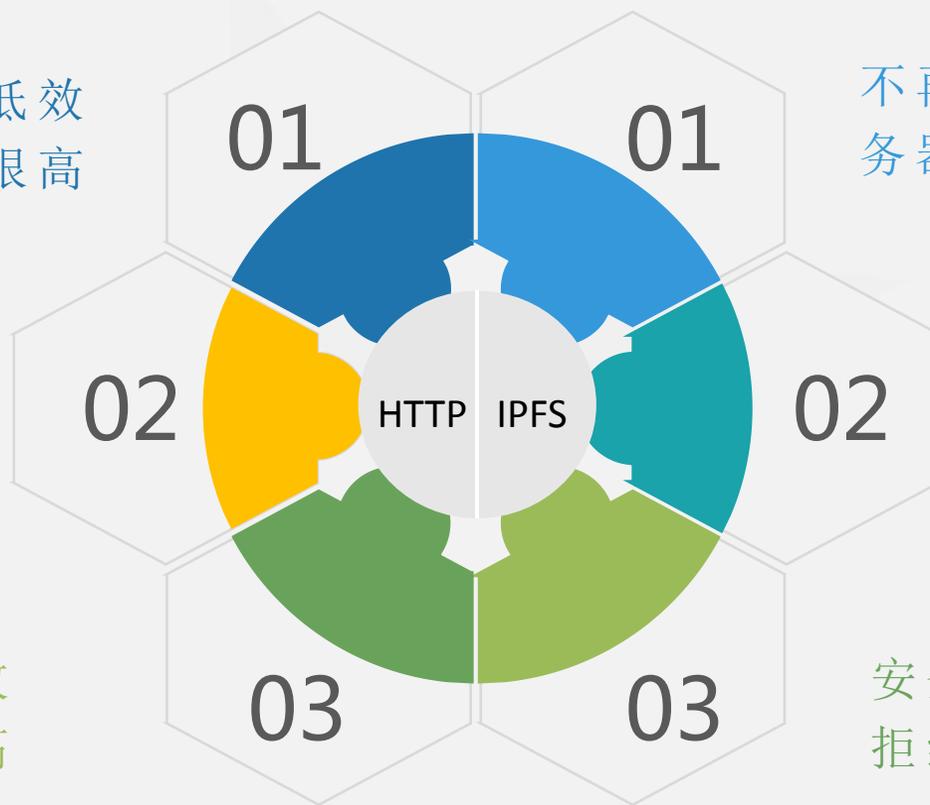
为什么需要IPFS?

众所周知，互联网是建立在HTTP协议上的。HTTP协议是个伟大的发明，让我们的互联网得以快速发展。但随着互联网的进步，HTTP逐渐显示出其不足之处。

HTTP存在中心化的低效
并且成本很高

Web文件经常被删除

极易受到攻击，防范攻击
成本高



不再依赖主干网和中心化服务器，
下载速度快

优化存储空间，数据
可持续保存

安全，天生抵御DDOS(分布式
拒绝服务攻击)攻击

IPFS与区块链的关系？



区块链

- 区块链存储效率低，成本高
- 跨链需要各个链之间协同配合，难以协调



IPFS

- 使用IPFS存储文件数据，并将唯一永久可用的IPFS地址放置到区块链中
- IPFS通过IPLD定义不同的分布式数据结构，协助各个链之间传递信息和文件

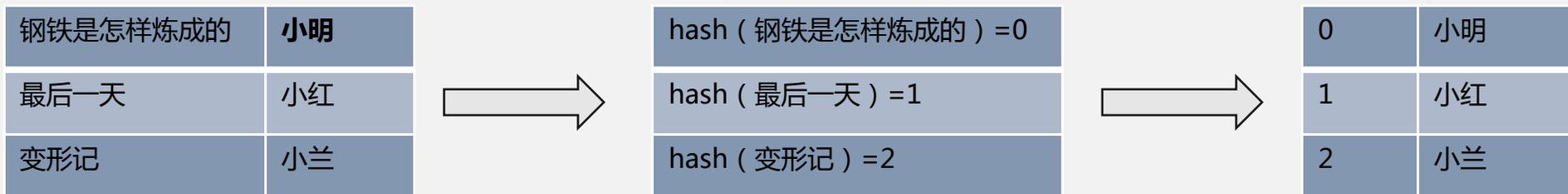
IPFS架构



IPFS特性—分布式哈希表(DHT)

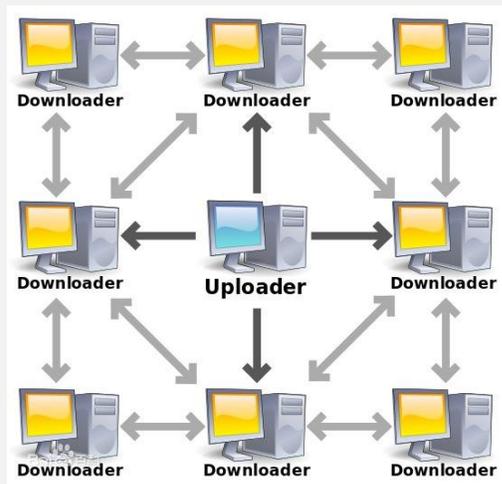
哈希表是一种数据结构，它把KEY 和 VALUE用某种方式对应起来。使用hash() 函数把一个KEY值映射到一个index上，即 $\text{hash}(\text{KEY}) = \text{index}$ 。这样就可以把一个KEY值同某个index对应起来。然后把与这个KEY值对应的VALUE存储到index所标记的存储空间中。这样，每次想要查找KEY所对应的VALUE值时，只需要做一次hash() 运算就可以找到了。

举个例子：图书馆中的书会被某人借走，这样“书名”和“人名”之间就形成了KEY与VALUE的关系。



IPFS特性—块交换协议 (BitTorrent)

仅仅实现数据的分布式存储还远远不够，数据还需要在节点之间有效的交换，从而使得整个系统能够高效运转。IPFS协议受BitTorrent 的启发，通过对等节点间交换数据块来分发数据。



如何激励节点分享数据？IPFS在BitTorrent的基础上进行了创新，增加了包括信用、策略、帐单在内的体系，这一体系之上的新的数据交换协议被称做BitSwap。

在BitSwap协议下，发送数据给其他节点可以增加节点信用值，而从其他节点接受数据则会降低节点信用值。也就是说，如果一个节点持续分享数据，其他节点给它发送数据的概率就会越来越大；而如果一个节点只接收数据而不分享数据，其他节点给它发送数据的概率就会越来越低，直到低到被其他节点忽略。

IPFS特性—自验证文件系统SFS

自验证文件系统（Self-Certifying File System, SFS）是为了设计一整套互联网共用的文件系统，全球的SFS系统都在同一个命名空间下。在SFS中，分享文件会变得十分简单，只需要提供文件名就行了。要实现一个全球共享的文件系统，最大的一个障碍莫过于如何让服务端为客户端提供认证。一个最简单的思路，所有服务器都生成一对公钥和私钥，然后让每个客户端用公开的公钥来验证服务器的安全，但是如何让所有客户端都能获得服务器的公钥呢？

SFS使用一种新的解决思路，将公钥信息嵌入到文件名中，这种命名为“自验证文件名”。这样就没必要在文件系统内部实现密钥管理了。密钥管理的功能就加入到用户对文件命名的规则中。用户可以根据自己需要选择加密方式。

IPFS的方案如下：

$\text{NodeID} = \text{hash}(\text{node.PubKey})$

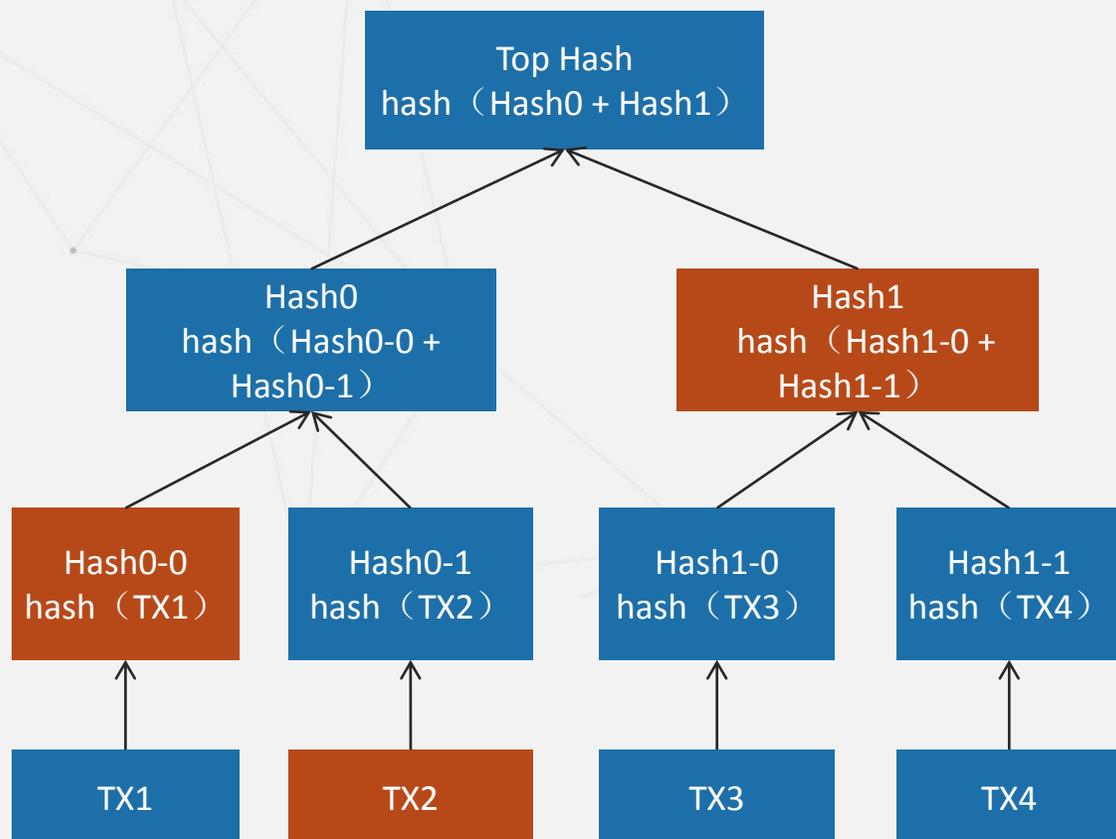
给每个用户分配一个可变的命名空间，在此路径下：`/ipns/`

一个用户可以在此路径下发布一个用自己私钥签名的对象，比如：`/ipns/XLF2ipQ4jD3UdeX5xp1KBgeHRhemUtaA8Vm/`

其他用户获取对象时，他们可检测签名是否与公钥和NodeID匹配，验证用户发布对象的真实性，达到了可变状态的获取。

IPFS特性-Merkle DAG

Merkle 树



IPFS中定义的Merkle DAG的对象格式

```
type IPFSObject struct {  
    links []IPFSLink // link数组  
    data []byte // 数据内容  
}  
  
type IPFSLink struct {  
    Name string // link的名字  
    Hash Multihash // 数据的加密哈希值  
    Size int // 数据大小  
}
```

Merkle DAG的特点：1、内容寻址 2、防篡改 3、去重

Filecoin: 基于IPFS技术的区块链项目

IPFS和Filecoin都是由协议实验室打造的明星项目，IPFS与Filecoin之间的关系有点类似于区块链与比特币的关系。Filecoin的诞生是为了通过经济激励的机制来促进IPFS的发展，Filecoin网络也需要IPFS为其市场的发展提供强大的生态支持。

Filecoin采用了区块链通证体系发行了Token，Token简称FIL，发行总量20亿，分配方案总共有四个部分组成：

- 1、矿工：70%（即14亿枚），通过区块奖励的方式线性释放，每6年减半；
- 2、团队：15%（即3亿枚），作为协议实验室团队的研发及运营费用，按6年线性释放；
- 3、投资人：10%（即2亿枚），分配给参与私募与公募的投资者，按6-36个月线性释放；
- 4、基金会：5%（即1亿枚），作为长期社区建设，网络管理等费用，按6年线性释放；

BSN中IPFS专网概述

BSN测试网IPFS专网面向应用开发提供IPFS常用的原生服务接口的服务网关，开发者可以无缝的与IPFS公网切换。为了让更多的开发者体验IPFS服务，我们对上传文件的大小限制为50M，并将根据存储资源的使用情况进行不定期重置清理，请不要将测试网用于生产环境。2021年1月31日发布的版本V1.4.0将包含BSN的IPFS专网商用功能。



如何在BSN中使用IPFS

➤ 方式一：在发布测试服务时开通。

测试网服务 / 发布测试服务

* 服务名称

* 版本号

* 平台类型

* 开通IPFS服务 是 否

➤ 方式二：在【我的IPFS服务】界面单独开通。

测试网服务

我的测试服务 我的IPFS服务

(IPFS服务为联盟链开发者提供上传Key、下载Key和节点网关接入的调试环境。IPFS服务将于2020-12-31进行重置，重置后所有的服务将删除)

创建IPFS服务 创建IPFS下载Key

暂未开通IPFS服务

IPFS实操—学习资料

- 1、书《IPFS原理与实践》
- 2、ipfs 命令手册<http://cw.hubwiz.com/card/c/ipfs/1/13/7/>
- 3、ipfs desktop <https://github.com/ipfs-shipyard/ipfs-desktop>



谢谢观看

