(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 108111585 A
(43)申请公布日 2018.06.01

(21)申请号 201711344195.1

(22)申请日 2017.12.15

(71)申请人 成都链一网络科技有限公司
地址 610000 四川省成都市高新区天华二路219号10栋19层

(72)发明人 尚小朋

(74)专利代理机构 成都厚为专利代理事务所（普通合伙）51255
代理人 夏柯双

(51)Int.Cl.
H04L 29/08(2006.01)
H04L 29/06(2006.01)
G06F 17/30(2006.01)

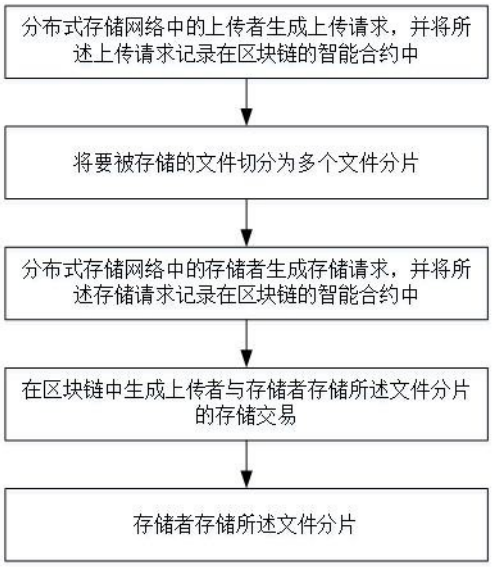
权利要求书1页 说明书4页 附图1页

(54)发明名称

基于区块链的分布式存储方法

(57)摘要

本发明公开了一种基于区块链的分布式存储方法，包括：S1.分布式存储网络中的上传者生成上传请求，并将所述上传请求记录在区块链的智能合约中；S2.将要被存储的文件切分为多个文件分片；S3.分布式存储网络中的存储者生成存储请求，并将所述存储请求记录在区块链的智能合约中；S4.在区块链中生成上传者与存储者存储所述文件分片的存储交易；S5.存储者存储所述文件分片。本发明实现了文件的分布式存储，提高了文件存储的安全性。



CN 108111585 A

1.基于区块链的分布式存储方法,其特征在于,包括:

S1.分布式存储网络中的上传者生成上传请求,并将所述上传请求记录在区块链的智能合约中;

S2.将要被存储的文件切分为多个文件分片;

S3.分布式存储网络中的存储者生成存储请求,并将所述存储请求记录在区块链的智能合约中;

S4.在区块链中生成上传者与存储者存储所述文件分片的存储交易;

S5.存储者存储所述文件分片。

2.根据权利要求1所述的基于区块链的分布式存储方法,其特征在于,所述上传请求包括文件的拆分数量、文件的备份数量、文件描述、上传者的公钥、上传者的账户名、上传者ID和文件ID。

3.根据权利要求1所述的基于区块链的分布式存储方法,其特征在于,所述存储请求包括存储者的账户名、文件ID和文件分片ID。

4.根据权利要求3所述的基于区块链的分布式存储方法,其特征在于,所述文件ID由所述文件的哈希值和上传者的公钥构成,所述文件分片ID由所述文件分片的哈希值和上传者的公钥构成。

5.根据权利要求1所述的基于区块链的分布式存储方法,其特征在于,所述S4包括:上传者查看所述存储请求,并为所述存储者授予存储所述文件分片的存储权限。

6.根据权利要求1所述的基于区块链的分布式存储方法,其特征在于,所述S5包括:

存储者向上传者发起下载所述文件分片的请求;

上传者验证存储者是否具有所述文件分片的存储权限,若是,则上传者允许存储者下载所述文件分片;

存储者从上传者处下载所述文件分片。

7.根据权利要求6所述的基于区块链的分布式存储方法,其特征在于,所述S5还包括:

存储者更新所述存储请求,写入所述文件分片下载完成的信息;

上传者更新所述上传请求,写入所述文件分片已存储的信息。

8.根据权利要求7所述的基于区块链的分布式存储方法,其特征在于,所述文件分片下载完成的信息包括文件ID、文件分片ID和存储者的账户名,所述文件分片已存储的信息包括上传者的账户名、文件ID、文件分片ID和存储者ID。

9.根据权利要求6所述的基于区块链的分布式存储方法,其特征在于,所述存储者与上传者之间通过电骡实现所述文件分片的传输。

基于区块链的分布式存储方法

技术领域

[0001] 本发明涉及数据存储技术领域,特别是涉及一种基于区块链的分布式存储方法。

背景技术

[0002] 现有技术中,数据存储有中心化存储方案和去中心化存储方案两种;目前,国际上有名的中心化存储方案有Dropbox、OneDrive、Google Drive和SkyDrive,国内较为成熟的中心化存储方案有百度网盘、华为网盘、金山快盘、115网盘、360云盘、坚果云和腾讯微云;去中心化存储方案比较著名的有Storj、Sia和Maidsafe。

[0003] 去中心化存储可以显著减小数据中断的风险及其损失,增加数据存储的安全性和保密性。现有云存储依赖于第三方大型存储商来传输和存储数据,如360云盘、百度网盘等,这些大型存储商拥有全部的数据备份以及所有的用户信息,受限于中心化的架构,非常容易受到各种安全威胁;冗余和去中心化的分布式存储可以有效改善这种状况,有效抵制篡改和未经授权的访问。

发明内容

[0004] 本发明的目的在于克服现有技术的不足,提供一种基于区块链的分布式存储方法,实现文件的分布式存储,提高文件存储的安全性。

[0005] 本发明的目的是通过以下技术方案来实现的:基于区块链的分布式存储方法,包括:

S1.分布式存储网络中的上传者生成上传请求,并将所述上传请求记录在区块链的智能合约中;

S2.将要被存储的文件切分为多个文件分片;

S3.分布式存储网络中的存储者生成存储请求,并将所述存储请求记录在区块链的智能合约中;

S4.在区块链中生成上传者与存储者存储所述文件分片的存储交易;

S5.存储者存储所述文件分片。

[0006] 优选的,所述上传请求包括文件的拆分数量、文件的备份数量、文件描述、上传者的公钥、上传者的账户名、上传者ID和文件ID。

[0007] 优选的,所述存储请求包括存储者的账户名、文件ID和文件分片ID。

[0008] 优选的,所述文件ID由所述文件的哈希值和上传者的公钥构成,所述文件分片ID由所述文件分片的哈希值和上传者的公钥构成。

[0009] 优选的,所述S4包括:上传者查看所述存储请求,并为所述存储者授予存储所述文件分片的存储权限。

[0010] 优选的,所述S5包括:

存储者向上传者发起下载所述文件分片的请求;

上传者验证存储者是否具有所述文件分片的存储权限,若是,则上传者允许存储者下

载所述文件分片；

存储者从上传者处下载并存储所述文件分片。

[0011] 优选的，所述S5还包括：

存储者更新所述存储请求，写入所述文件分片下载完成的信息；

上传者更新所述上传请求，写入所述文件分片已存储的信息。

[0012] 优选的，所述文件分片下载完成的信息包括文件ID、文件分片ID和存储者的账户名，所述文件分片已存储的信息包括上传者的账户名、文件ID、文件分片ID和存储者ID。

[0013] 优选的，所述存储者与上传者之间通过电骡实现所述文件分片的传输。

[0014] 本发明的有益效果是：

(1)本发明实现了文件的分布式存储，任何一个节点都不会拥有整个文件的完整备份，提高了文件的安全性；

(2)将文件的元数据等重要信息通过智能合约验证存储在区块链中，由于存储在区块链中的数据不可能被篡改，因此使得这些重要信息能够得到很好的保护；

(3)每个用户既可以是存储需求方，也可以是存储提供方，能够有效提高网络中用户闲散的存储资源的利用率，同时也为提供存储资源的用户带来相应的收益；

(4)采用电骡进行文件分片的传输，稳定性良好。

附图说明

[0015] 图1为本发明的流程示意图。

具体实施方式

[0016] 下面将结合实施例，对本发明的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域技术人员在没有付出创造性劳动的前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0017] 术语解释：

区块链：一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构，并以密码学方式保证的不可篡改和不可伪造的分布式账本。

[0018] 智能合约：一套以数字形式定义的承诺，包括合约参与方可以执行这些承诺的协议。从程序角度来看，智能合约是编程在区块链上的程序语言，当满足某些指定条件时触发相关操作。

[0019] 参阅图1，本实施例提供了一种基于区块链的分布式存储方法，具体包括以下步骤：

S1.分布式存储网络中的上传者生成上传请求，并将所述上传请求记录在区块链的智能合约中。

[0020] 所述上传请求包括所述文件的拆分数量、所述文件的备份数量、付费意愿、文件描述、上传者的公钥、上传者的账户名、上传者ID、文件ID。所述文件ID由所述文件的哈希值和上传者的公钥构成。

[0021] 上传者为分布式存储网络中作为存储需求方的用户，即该用户有文件需要被存

储。上传者发起上传文件到分布式存储网络的请求，对该请求进行基本的校验后设置相关参数，然后调用区块链的File_Upload(文件上传)合约的Upload(上传)接口的交易，合约校验没有问题后在区块链上为其创建一个上传请求(Upload Request)记录。

[0022] S2.将要被存储的文件切分为多个文件分片。即根据上传请求中文件的拆分数量和备份数量将文件切分为多个文件分片；例如，文件的拆分数量为5，备份数量为2，即将文件拆分成5个文件分片，每个文件分片有两个副本，一共有十个文件分片需要进行存储。

[0023] 在将文件切分为多个文件分片后，将所述文件分片存储至上传者设定的位置。

[0024] S3.分布式存储网络中的存储者生成存储请求，并将所述存储请求记录在区块链的智能合约中。

[0025] 所述存储请求包括存储者的账户名、文件ID和文件分片ID；所述文件ID由所述文件的哈希值和上传者的公钥构成，所述文件分片ID由所述文件分片的哈希值和上传者的公钥构成。

[0026] 存储者为分布式存储网络中作为存储资源提供方的用户，即该用户为上传者提供存储资源。存储者调用区块链的blockchain_get__upload_requests接口(查看存在的上传请求)查看上传者的上传请求，存储者在看到上传请求后，将所述文件的哈希值和上传者的公钥组合形成文件ID，生成存储请求，声明自己想要存储该文件的哪些文件分片。

[0027] S4.在区块链中生成上传者与存储者存储所述文件分片的存储交易。即，上传者查看所述存储请求，并为所述存储者授予存储所述文件分片的存储权限。

[0028] 上传者调用区块链的wallet_list_store_request_for_my_file(存储请求查看接口，用于上传者查看与自己要上传的文件相关的存储请求)接口查看存储者的存储请求，然后，上传者调用区块链的wallet_allow_store_request接口(允许下载接口用于为存储者授予某一文件分片的存储权限)来允许存储者存储相应的文件分片(即允许存储者下载相应的文件分片)。

[0029] S5.存储者存储所述文件分片。

[0030] 所述S5包括：存储者向上传者发起下载所述文件分片的请求；上传者验证存储者是否具有所述文件分片的存储权限，若是，则上传者允许存储者下载所述文件分片；存储者从上传者处下载并存储所述文件分片。

[0031] 存储者的电骡给上传者的电骡发送下载相应文件分片的请求，上传者的电骡收到该请求后调用区块链的download_validation(鉴权接口，用于进行下载权限鉴定)来验证是否允许存储者下载。如果允许，则存储者的电骡从上传者的电骡下载相应的文件分片。

[0032] 所述S5还包括：存储者更新所述存储请求，写入所述文件分片下载完成的信息；上传者更新所述上传请求，写入所述文件分片已存储的信息。

[0033] 所述文件分片下载完成的信息包括文件ID、文件分片ID和存储者的账户名，所述文件分片已存储的信息包括上传者的账户名、文件ID、文件分片ID和存储者ID。

[0034] 存储者的电骡下载完成后，存储者调用区块链的declare_piece_saved(存储完成声明接口，用于存储者发起已完成某一文件分片存储的声明)，在区块链上写入“该文件分片下载完成”的状态，上传者调用区块链的blockchain_list_file_save_declare(存储完成声明查看接口，用于列出区块链网络中出现的与指定文件相关的存储完成声明)接口查询自己要上传的文件的存储状态信息，上传者查看到该文件的某个文件分片已被存储后，

调用区块链的confirm_piece_saved(确认存储声明接口,用于上传者发起已确认存储者完成某一文件分片的存储的声明),在区块链上写入“该文件分片已存储”的状态。当所述文件的所有文件分片被存储者下载完成后,即完成所述文件的存储。

[0035] 以上所述仅是本发明的优选实施方式,应当理解本发明并非局限于本文所披露的形式,不应看作是对其他实施例的排除,而可用于各种其他组合、修改和环境,并能够在本文所述构想范围内,通过上述教导或相关领域的技术或知识进行改动。而本领域人员所进行的改动和变化不脱离本发明的精神和范围,则都应在本发明所附权利要求的保护范围内。

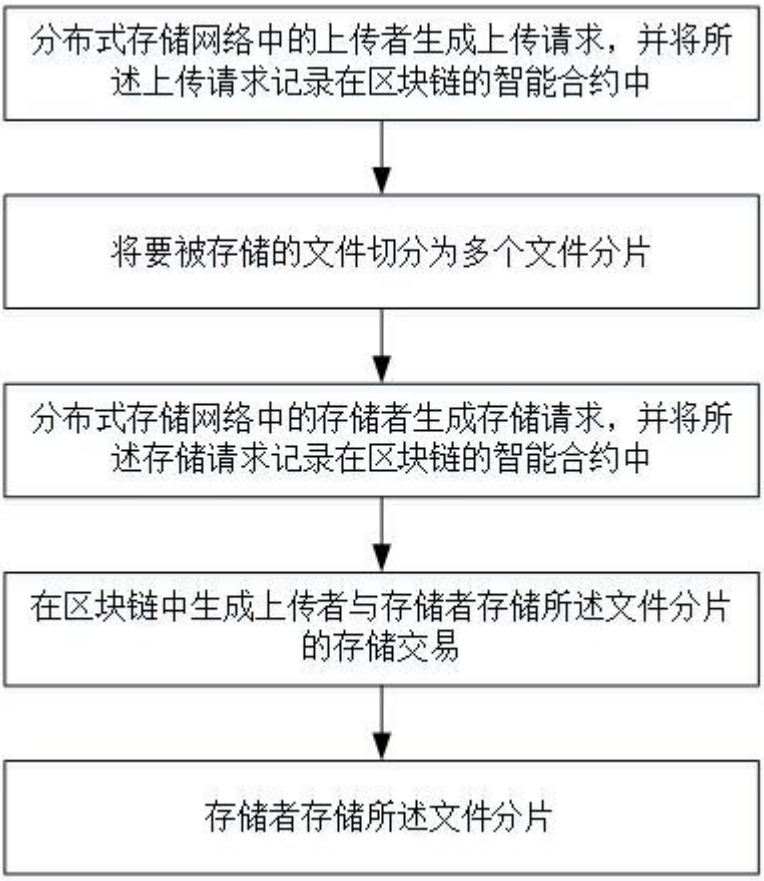

分布式存储网络中的上传者生成上传请求，并将所述上传请求记录在区块链的智能合约中
将要被存储的文件切分为多个文件分片
分布式存储网络中的存储者生成存储请求，并将所述存储请求记录在区块链的智能合约中
在区块链中生成上传者与存储者存储所述文件分片的存储交易
存储者存储所述文件分片

图1