(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 108076148 A
(43)申请公布日 2018.05.25

(21)申请号 201711344107.8

(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)

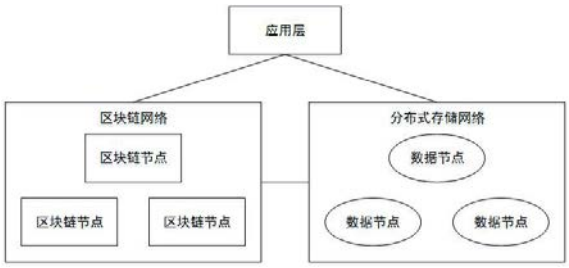
权利要求书1页 说明书5页 附图1页

(54)发明名称

基于区块链的存储系统

(57)摘要

本发明公开了一种基于区块链的存储系统，包括：应用层，用于上传者生成上传请求、存储者生成存储请求和下载者生成下载请求，以及根据所述上传请求将要被存储的文件切分为多个文件分片；区块链网络，用于存储所述上传请求、下载请求和文件的元信息，以及用于对发起下载请求的下载者进行权限验证；分布式存储网络，用于存储所述文件分片，以及在上传文件时对存储者进行权限验证、在下载文件时对下载者进行权限验证。本发明采用区块链技术将文件的元信息存储在区块链网络中，使其不能被篡改，大大提高了安全性，再结合电骡网络提供的稳定性，实现了稳定安全的云存储。



CN 108076148 A

1.基于区块链的存储系统,其特征在于,包括:

应用层,用于上传者生成上传请求、存储者生成存储请求和下载者生成下载请求,以及根据所述上传请求将要被存储的文件切分为多个文件分片;

区块链网络,用于存储所述上传请求、下载请求和文件的元信息,以及用于对发起下载请求的下载者进行权限验证;

分布式存储网络,用于存储所述文件分片,以及在上传文件时对存储者进行权限验证、在下载文件时对下载者进行权限验证。

2.根据权利要求1所述的基于区块链的存储系统,其特征在于,所述分布式存储网络为Kad分布式存储网络。

3.根据权利要求1所述的基于区块链的存储系统,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,所述存储请求包括存储者的账户名、文件ID和文件分片ID,所述下载请求包括下载者的账户名和文件ID。

4.根据权利要求1所述的基于区块链的存储系统,其特征在于,所述文件的元信息包括文件的分片信息、上传者的公钥和存储者ID。

5.根据权利要求1所述的基于区块链的存储系统,其特征在于,所述区块链网络为支持智能合约的区块链网络。

6.根据权利要求1所述的基于区块链的存储系统,其特征在于,所述区块链网络包括:

上传请求发起接口,用于上传者发起将文件存储到分布式存储网络的上传请求;

上传请求查看接口,用于存储者查看区块链网络中存在的所有上传请求;

存储请求发起接口,用于存储者发起存储某一文件分片的存储请求;

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;

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;

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;

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;

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;

鉴权接口,用于进行下载权限鉴定;

下载请求接口,用于下载者发起获取某一文件的访问权的请求。

7.根据权利要求6所述的基于区块链的存储系统,其特征在于,所述上传请求发起接口用于发起调用文件上传合约的上传接口的交易,该合约检验无误后为上传者在区块链网络中创建一个上传请求记录;

所述存储请求接口,用于发起调用文件上传合约的存储接口的交易,该合约校验无误后为存储者在区块链网络中创建一个存储请求记录;

所述下载请求接口用于发起调用文件上传合约的获取接口的交易,该合约根据上传者设定的鉴权条件判断是否允许所述下载者访问所述文件,若是,则在区块链网络中为下载者创建一个访问许可记录。

8.根据权利要求1所述的基于区块链的存储系统,其特征在于,存储者与上传者之间、存储者与下载者之间均通过电骡进行传输。

基于区块链的存储系统

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存储系统。

背景技术

[0002] 云存储是在云计算(cloud computing)概念上延伸和发展出来的一个新的概念,是一种新兴的网络存储技术,是指通过集群应用、网络技术或分布式文件系统等功能,将网络中大量各种不同类型的存储设备通过应用软件集合起来协同工作,共同对外提供数据存储和业务访问功能的系统。

[0003] 当云计算系统运算和处理的核心是大量数据的存储和管理时,云计算系统中就需要配置大量的存储设备,那么云计算系统就转变成为一个云存储系统,所以云存储是一个以数据存储和管理为核心的云计算系统。简单来说,云存储就是将储存资源放到云上供人存取的一种新兴方案。使用者可以在任何时间、任何地方,透过任何可连网的装置连接到云上方便地存取数据。

[0004] 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。

发明内容

[0005] 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存储系统,实现文件的分布式存储,提高文件存储的安全性。

[0006] 本发明的目的是通过以下技术方案来实现的:基于区块链的存储系统,包括:

应用层,用于上传者生成上传请求、存储者生成存储请求和下载者生成下载请求,以及根据所述上传请求将要被存储的文件切分为多个文件分片;

区块链网络,用于存储所述上传请求、下载请求和文件的元信息,以及用于对发起下载请求的下载者进行权限验证;

分布式存储网络,用于存储所述文件分片,以及在上传文件时对存储者进行权限验证、在下载文件时对下载者进行权限验证。

[0007] 优选的,所述分布式存储网络为Kad分布式存储网络。

[0008] 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,所述存储请求包括存储者的账户名、文件ID和文件分片ID,所述下载请求包括下载者的账户名和文件ID。

[0009] 优选的,所述文件的元信息包括文件的分片信息、上传者的公钥和存储者ID。

[0010] 优选的,所述区块链网络为支持智能合约的区块链网络。

优选的,所述区块链网络包括:

上传请求发起接口,用于上传者发起将文件存储到分布式存储网络的上传请求;

上传请求查看接口,用于存储者查看区块链网络中存在的所有上传请求;

存储请求发起接口，用于存储者发起存储某一文件分片的存储请求；

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；

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；

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；

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；

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；

鉴权接口，用于进行下载权限鉴定；

下载请求接口，用于下载者发起获取某一文件的访问权的请求。

[0011] 优选的，所述上传请求发起接口用于发起调用文件上传合约的上传接口的交易，该合约检验无误后为上传者在区块链网络中创建一个上传请求记录；

所述存储请求接口，用于发起调用文件上传合约的存储接口的交易，该合约校验无误后为存储者在区块链网络中创建一个存储请求记录；

所述下载请求接口用于发起调用文件上传合约的获取接口的交易，该合约根据上传者设定的鉴权条件判断是否允许所述下载者访问所述文件，若是，则在区块链网络中为下载者创建一个访问许可记录。

[0012] 优选的，存储者与上传者之间、存储者与下载者之间均通过电骡进行传输。

[0013] 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)本发明基于电骡底层进行开发，在一个已验证的可靠网络的基础上设计出的架构也具有同样的优势；同时，由于电骡时基于点对点的分布式文件分析，本发明则是分布式网络存储，其本质目的区别于电骡，而且，本发明采用区块链技术将文件的元信息存储在区块链网络中，以分布式账本的形式对文件的元信息进行保存，使其不能被篡改，大大提高了安全性，再结合电骡网络提供的稳定性，实现了稳定安全的云存储；

(5)本发明中进行文件下载时设有多重验证，进一步提高了安全性。

附图说明

[0014] 图1为本发明的示意框图。

具体实施方式

[0015] 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。

[0016] 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。

[0017] 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。

[0018] 参阅图1，本实施例提供一种基于区块链的存储系统：基于区块链的存储系统在于包括应用层、区块链网络和分布式存储网络。

[0019] 所述应用层用于上传者生成上传请求、存储者生成存储请求和下载者生成下载请求，以及根据所述上传请求将要被存储的文件切分为多个文件分片。

[0020] 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，此外，还可以包括下载者的鉴权条件；所述存储请求包括存储者的账户名、文件ID和文件分片ID；所述下载请求包括下载者的账户名和文件ID。

[0021] 所述区块链网络用于存储所述上传请求、下载请求和文件的元信息，以及用于对发起下载请求的下载者进行权限验证。

[0022] 所述文件的元信息包括文件的分片信息、上传者的公钥和存储者ID。所述区块链网络为支持智能合约的区块链网络。

[0023] 所述区块链网络包括上传请求发起接口、上传请求查看接口、存储请求发起接口、存储请求查看接口、允许下载接口、存储完成声明接口、存储完成声明查看接口、确认存储声明接口、鉴权接口和下载请求接口。

[0024] 所述上传请求发起接口(store_file_to_network)用于上传者发起将文件存储到分布式存储网络的上传请求；在一些实施例中，实现过程为：发起调用文件上传(File_Upload)合约的上传(Upload)接口的交易，该合约检验无误后为上传者在区块链网络中创建一个上传请求(Upload Request)记录。

[0025] 所述上传请求查看接口(blockchain_get_upload_requests)，用于存储者查看区块链网络中存在的所有上传请求。

[0026] 所述存储请求发起接口(store_file_piece)，用于存储者发起存储某一文件分片的存储请求；在一些实施例中，实现过程为：发起调用文件上传(File_Upload)合约的存储(Store)接口的交易，该合约校验无误后为存储者在区块链网络中创建一个存储请求(Store Request)记录。

[0027] 所述存储请求查看接口(wallet_list_store_request_for_my_file)，用于上传者查看与自己要上传的文件相关的存储请求；在一些实施例中，实现过程为：根据上传请求从区块链网络中取出相关的存储请求，此接口根据文件分片ID查询区块链网络中的数据，列出相关存储请求信息。

[0028] 所述允许下载接口(wallet_allow_store_request)，用于为存储者授予某一文件分片的存储权限；在一些实施例中，实现过程为：在区块链网络中记录下许可的存储请求，使得在下载鉴权时可以通过。

[0029] 所述存储完成声明接口(declare_piece_saved)，用于存储者发起已完成某一文件分片存储的声明；在一些实施例中，实现过程为：发起一笔交易，交易中包含一个指定账

户已完成特定文件分片存储的声明。

[0030] 所述存储完成声明查看接口(blockchain_list_file_save_declare),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。

[0031] 所述确认存储声明接口(confirm_piece_saved),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;

所述鉴权接口(download_validation),用于进行下载权限鉴定,判断存储者或下载者是否有权下载相应的文件分片。

[0032] 所述下载请求接口(get_file_access),用于下载者发起获取某一文件的访问权的请求;在一些实施例中,实现过程为:发起调用文件上传合约的获取接口的交易,该合约根据上传者设定的鉴权条件判断是否允许所述下载者访问所述文件,若是,则在区块链网络中为下载者创建一个访问许可记录。

[0033] 分布式存储网络,用于存储所述文件分片,以及在上传文件时对存储者进行权限验证、在下载文件时对下载者进行权限验证。

[0034] 所述分布式存储网络为Kad分布式存储网络。

[0035] 上传者、存储者和下载者均为分布式存储网络在的节点,存储者与上传者之间、存储者与下载者之间均通过电骡进行传输。

[0036] 本实施例中的存储系统的上传和下载过程为:

S1.上传者调用上传请求发起接口(store_file_to_network)生成上传请求,并将所述上传请求记录在区块链网络的智能合约中;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。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。

[0037] S2.存储者调用区块链网络的上传请求查看接口(blockchain_get__upload_requests)查看上传者的上传请求。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。

[0038] S3. 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,通过存储请求发起接口(store_file_piece)生成存储请求,声明自己想要存储该文件的哪些文件分片。

[0039] S4.上传者调用区块链网络的存储请求查看接口(wallet_list_store_request_for_my_file)查看存储者的存储请求。

[0040] S5.上传者调用区块链网络的允许下载接口(wallet_allow_store_request)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)。

[0041] S6.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网络的鉴权接口(download_validation)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。

[0042] S7.存储者的电骡下载完成后,存储者调用区块链网络的存储完成声明接口(declare_piece_saved),在区块链上写入“该文件分片下载完成”的状态。

[0043] S8.上传者调用区块链网络的存储完成声明查看接口(blockchain_list_file_

save_declare)查询自己要上传的文件的存储状态信息。

[0044] S9. 上传者查看到该文件的某个文件分片已被存储后,调用区块链网络的确认存储声明接口(confirm_piece_saved),在区块链网络上写入“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。

[0045] 操作:文件下载

S10.下载者从区块链网络中查看已经确认存储的文件。

[0046] S11.下载者调用区块链网络的下载请求接口(get_file_access)发起下载请求,该下载请求接口调用文件上传(File_Upload)合约的访问接口(Access),合约根据文件的上传者设定的鉴权合约判断是否应当许可下载者访问文件,若是,则在区块链网络中为下载者创建访问许可记录。

[0047] S12.下载者的电骡给相应存储者的电骡发各个文件分片的文件下载请求,存储者的电骡收到该下载请求后,调用区块链网络的鉴权接口(download_validation)来验证是否允许下载者下载所述文件分片,若是,则下载者的电骡从存储者的电骡下载所述文件分片。

[0048] S13.下载者从存储者处下载完文件的所有文件分片后,将所有文件分片拼装成完整的文件,下载流程完成。

[0049] 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。

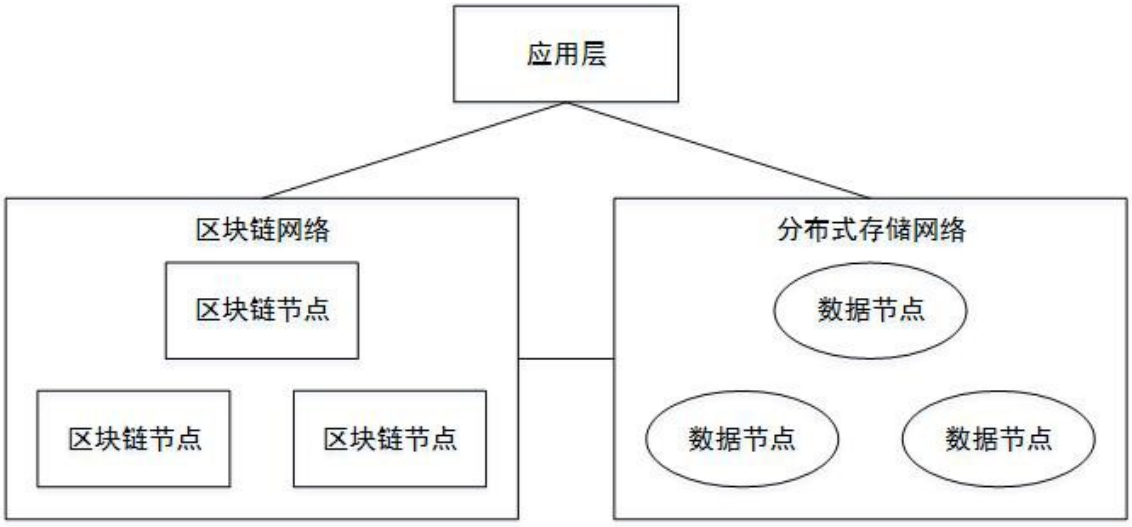


图1