(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 107770154 A
(43)申请公布日 2018.03.06

(21)申请号 201710866747.9

(22)申请日 2017.09.22

(71)申请人 中国科学院信息工程研究所
地址 100093 北京市海淀区闵庄路甲89号

(72)发明人 张锐 肖禹亭 马晖

(74)专利代理机构 北京路浩知识产权代理有限公司 11002
代理人 王莹 李相雨

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

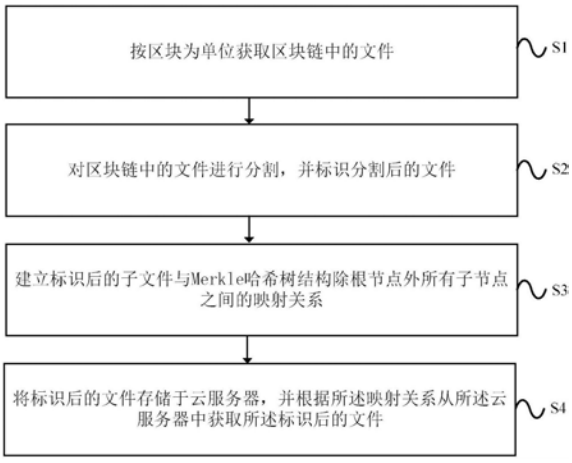
权利要求书2页 说明书11页 附图3页

(54)发明名称

基于云存储的区块链可靠数据存储方法、终端及系统

(57)摘要

本发明实施例提供一种基于云存储的区块链可靠数据存储方法、终端及系统，所述方法包括：按区块为单位获取区块链中的文件；对区块链中的文件进行分割，并标识分割后的文件；建立标识后的子文件与Merkle哈希树结构除根节点外所有子节点之间的映射关系；将标识后的文件存储于云服务器，并根据所述映射关系从所述云服务器中获取所述标识后的文件。所述终端执行上述方法。所述系统包括上述终端和云服务器。本发明实施例提供的基于云存储的区块链可靠数据存储方法、终端和系统，将数据外包存储至云服务器，终端可周期性地审计数据的完整性。



CN 107770154 A

1.一种基于云存储的区块链可靠数据存储方法,其特征在于,包括:

按区块为单位获取区块链中的文件;

对区块链中的文件进行分割,并标识分割后的文件;

建立标识后的子文件与Merkle哈希树结构除根节点外所有子节点之间的映射关系;

将标识后的文件存储于云服务器,并根据所述映射关系从所述云服务器中获取所述标识后的文件。

2.根据权利要求1所述的方法,其特征在于,所述方法还包括:

在所述将标识后的文件存储于云服务器的步骤之后,对标识后的文件进行文件完整性的验证;

和/或,

在所述并根据所述映射关系从所述云服务器中获取所述标识后的文件的步骤之后,将标识后的文件下载到所述区块链的本地节点。

3.根据权利要求2所述的方法,其特征在于,所述对标识后的文件进行文件完整性的验证,包括:

随机选取待检测文件并获取其被分割的子文件数m和所述待检测文件的标识;

根据所述子文件数m和第一预设规则,生成L组随机变量;

向云服务器发送数据查询请求,所述数据查询请求携带有所述L组随机变量,以供所述云服务器根据预先存储的文件分割后子文件的标签、所述数据查询请求和第二预设规则,获取反映待检测文件完整性的计算结果;其中,$1 \leqslant L \leqslant m$;

接收所述云服务器返回的所述计算结果,并根据所述计算结果、所述L组随机变量、所述标识、预先获得的秘钥和第三预设规则,验证所述待检测文件完整性。

4.根据权利要求3所述的方法,其特征在于,所述根据所述子文件数m和第一预设规则,生成L组随机变量,包括:

在所述m个子文件中随机选择L个子文件;

生成与每一个子文件标识i_j一一对应的随机数c_j,所述随机数的取值范围在预设的有限域之内;

将所述子文件标识i_j和所述随机数c_j两两组合,以获取L组随机变量$\{i_j,c_j\}$,其中,$1 \leqslant j \leqslant L$。

5.根据权利要求3所述的方法,其特征在于,预先获得的秘钥包括第一秘钥K1和第二秘钥K2,相应的;所述根据所述计算结果、所述L组随机变量、所述标识、预先获得的秘钥和第三预设规则,验证所述待检测文件完整性,包括:

将所述第一秘钥K1输入第一预设函数,以获取向量元素数为n的向量u;

将所述向量u与所述计算结果中的第一子文件向量w进行内积运算,以获取内积运算结果a;

将所述第二秘钥K2、所述标识和所述L组随机变量中的子文件标识i_j输入第二预设函数,以获取中间计算结果$H(K2,(id,i_j))$,其中,id为所述标识,i_j为子文件标识;

根据所述中间计算结果$H(K2,(id,i_j))$和所述L组随机变量中的随机数c_j获取中间参数b;

根据所述内积运算结果a、所述中间参数b和所述计算结果中的第二子文件向量t,验证

所述待检测文件完整性。

6.根据权利要求5所述的方法，其特征在于，根据所述中间计算结果H(K2,(id,i_j))和所述L组随机变量中的随机数c_j获取中间参数b，包括：

根据如下公式获取中间参数b：

$$b=\sum_{j=1}^{L}c_j\cdot[H(K2,(id,i_j))];$$

其中，c_j为L组随机变量中的随机数、H为第二预设函数、K2为第二秘钥、id为所述标识、i_j为子文件标识、$1\leqslant j\leqslant L$。

7.根据权利要求5所述的方法，其特征在于，所述根据所述内积运算结果a、所述中间参数b和所述第二子文件向量t，验证所述待检测文件完整性，包括：

将内积运算结果a和中间参数b进行相加；

若相加结果等于所述第二子文件向量t，则验证所述待检测文件完整性为完整；

或，

若相加结果不等于所述第二子文件向量t，则验证所述待检测文件完整性为不完整。

8.根据权利要求3至7任一所述的方法，其特征在于，在获取待检测文件被分割的子文件数m和所述待检测文件的标识的步骤之前，所述方法还包括：

分别指定所有文件中的每一个文件的标识；

将所述每一个文件平均分成m份，并进行向量化，以获取向量集合vi；

将随机生成的第一秘钥K1输入第一预设函数，以获取向量元素数为N的向量u；

将随机生成的第二秘钥K2、所述每一个文件的标识和m个子文件中的每一个子文件i输入第二预设函数H，以获取m个计算值b_i；

将向量u和所述向量集合vi进行内积运算，以获取m个计算结果；

将m个计算结果中的每一个与每一个计算值b_i分别相加，相加的结果作为ti；

将结果(vi,ti)和所述每一个文件的标识作为子文件的标签，并发送至云服务器，以供所述云服务器根据所述子文件的标签，获取待检测文件中的子文件信息(vi_j,ti_j)。

9.一种基于云存储的区块链可靠数据存储终端，其特征在于，包括：

获取单元，用于按区块为单位获取区块链中的文件；

标识单元，用于对区块链中的文件进行分割，并标识分割后的文件；

建立单元，用于建立标识后的子文件与Merkle哈希树结构除根节点外所有子节点之间的映射关系；

存储单元，用于将标识后的文件存储于云服务器，并根据所述映射关系从所述云服务器中获取所述标识后的文件。

10.一种基于云存储的区块链可靠数据存储系统，其特征在于，所述系统包括终端和云服务器。

基于云存储的区块链可靠数据存储方法、终端及系统

技术领域

[0001] 本发明实施例涉及计算机应用技术领域，具体涉及一种基于云存储的区块链可靠数据存储方法、终端及系统。

背景技术

[0002] 区块链技术的出现推动了无中心电子货币、分布式账本以及一系列以区块链为基础的分布式应用等的发展。然而现有的区块链技术仅要求节点在本地存储数据备份，没有提供任何一种机制保证在全网中一定存在某一个区块。一旦出现设备故障、人为误操作、自然灾害等突发情况，数据可能被损坏甚至永久性地丢失。这导致了现有的区块链技术不能够适用于需要可靠存储的应用场景。

[0003] 因此，如何保证区块链数据的完整性成为亟待解决的问题。

发明内容

[0004] 针对现有技术存在的问题，本发明实施例提供一种基于云存储的区块链可靠数据存储方法、终端及系统。

[0005] 第一方面，本发明实施例提供一种基于云存储的区块链可靠数据存储方法，所述方法包括：

[0006] 按区块为单位获取区块链中的文件；

[0007] 对区块链中的文件进行分割，并标识分割后的文件；

[0008] 建立标识后的子文件与Merkle哈希树结构除根节点外所有子节点之间的映射关系；

[0009] 将标识后的文件存储于云服务器，并根据所述映射关系从所述云服务器中获取所述标识后的文件。

[0010] 第二方面，本发明实施例提供一种基于云存储的区块链可靠数据存储终端，所述终端包括：

[0011] 获取单元，用于按区块为单位获取区块链中的文件；

[0012] 标识单元，用于对区块链中的文件进行分割，并标识分割后的文件；

[0013] 建立单元，用于建立标识后的子文件与Merkle哈希树结构除根节点外所有子节点之间的映射关系；

[0014] 存储单元，用于将标识后的文件存储于云服务器；

[0015] 下载单元，用于在指定需要下载的数据后根据所述映射关系从所述云服务器中获取相应的标识后的文件，并进行下载到本地；

[0016] 验证单元，用于对存储于云服务器上的标识后的文件进行文件完整性的验证。

[0017] 第三方面，本发明实施例提供一种基于云存储的区块链可靠数据存储系统，所述文件存储系统包括终端和云服务器。

[0018] 本发明实施例提供的基于云存储的区块链可靠数据存储方法、终端和系统，将数

据外包存储至云服务器，终端可周期性地审计数据的完整性。

附图说明

[0019] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作一简单地介绍，显而易见地，下面描述中的附图是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0020] 图1为本发明实施例基于云存储的区块链可靠数据存储方法流程示意图；

[0021] 图2为本发明实施例基于云存储的区块链可靠数据存储系统数据结构图；

[0022] 图3为本发明另一实施例基于云存储的区块链可靠数据存储方法流程示意图；

[0023] 图4为本发明实施例基于云存储的区块链可靠数据存储系统流程图；

[0024] 图5为本发明实施例基于云存储的区块链可靠数据存储终端结构示意图；

[0025] 图6为本发明实施例基于云存储的区块链可靠数据存储系统结构示意图；

[0026] 图7为本发明实施例提供的终端实体结构示意图。

具体实施方式

[0027] 为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例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，本领域普通技术人员在没有作出创造性劳动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。

[0028] 图1为本发明实施例基于区块链的文件存储方法流程示意图，如图1所示，本发明实施例提供的一种基于区块链的文件存储方法，包括以下步骤：

[0029] S1：按区块为单位获取区块链中的文件。

[0030] 具体的，终端按区块为单位获取区块链中的文件。这里的终端不限于本地终端和移动终端，该文件特指区块封装的交易数据集，利用该数据集构成的Merkle哈希树的根节点可以实现快速验证某个特定的数据存在于该区块中。

[0031] 特别地，当区块链中产生新区块时，本步骤会被触发。

[0032] S2：对区块链中的文件进行分割，并标识分割后的文件。

[0033] 具体的，终端对区块链中的文件进行分割，并标识分割后的文件。图2为本发明实施例区块链系统数据结构图，如图2所示，文件被分割后，需要对分割后的文件进行标识，例如可以采用ID号：F1～F7分别作为分割后文件中的每一个子文件的标识。

[0034] S3：建立标识后的子文件与Merkle哈希树结构除根节点外所有子节点之间的映射关系。

[0035] 具体的，终端建立标识后的子文件与Merkle哈希树结构除根节点外所有子节点之间的映射关系。映射关系可以是F1对应D1、F2对应D2等一一对应的关系，但不作具体限定。特别地，区块链技术采用Merkle哈希树结构是为了提供快速验证某个数据存在于某个区块的机制。如图2所示，Merkle哈希树结构中D1～D4为区块链需要封装的交易数据本身对应的哈希值，D5～D6为两两哈希后的中间值，D7为Merkle根。为了减少云服务器的计算开销，除Merkle根外其余所有数据均需要被存储在云服务器上。

[0036] S4:将标识后的文件存储于云服务器,并根据所述映射关系从所述云服务器中获取所述标识后的文件。

[0037] 具体的,终端将标识后的文件存储于云服务器,并根据所述映射关系从所述云服务器中获取所述标识后的文件。由于可周期性地对标识后的文件进行完整性审计,可保证文件的存储可靠性。通过上述的映射关系可以从云服务器中获取原文件。

[0038] 本发明实施例提供的基于云存储的区块链可靠数据存储方法,将数据外包存储至云服务器,终端可周期性地审计数据的完整性。

[0039] 在上述实施例的基础上,所述方法还包括:

[0040] 在所述将标识后的文件存储于云服务器的步骤之后,对标识后的文件进行文件完整性的验证。

[0041] 具体的,终端在所述将标识后的文件存储于云服务器的步骤之后,对标识后的文件进行文件完整性的验证。

[0042] 和/或,

[0043] 在所述并根据所述映射关系从所述云服务器中获取所述标识后的文件的步骤之后,将标识后的文件下载到所述区块链的本地节点。

[0044] 具体的,终端在所述并根据所述映射关系从所述云服务器中获取所述标识后的文件的步骤之后,将标识后的文件下载到所述区块链的本地节点。可以对存储于云服务器中的文件进行完整性的验证和下载到本地等,但不作具体限定。

[0045] 本发明实施例提供的基于云存储的区块链可靠数据存储方法,能够进行文件完整性的验证和下载到区块链的本地节点。

[0046] 在上述实施例的基础上,所述对标识后的文件进行文件完整性的验证,包括:

[0047] 随机选取待检测文件并获取其被分割的子文件数m和所述待检测文件的标识。

[0048] 具体的,终端随机选取待检测文件并获取其被分割的子文件数m和所述待检测文件的标识。随机选取待检测文件,即随机选取区块链的一个区块作为待检测区块,根据该区块中存储的数据对应表,获取所述待检测文件被分割后的子文件数m,m可以等于7(对应图2中的F1-F7):待检测文件的标识用于区分不同的待检测文件,对应图2中的区块序列号。

[0049] 根据所述子文件数m和第一预设规则,生成L组随机变量。

[0050] 具体的,终端根据所述子文件数m和第一预设规则,生成L组随机变量。对生成L组随机变量详细说明如下:

[0051] 在m个子文件中选择L个子文件;

[0052] 生成与每一个子文件标识i_j一一对应的随机数c_j,随机数的取值范围在预设的有限域之内;

[0053] 将子文件标识i_j和随机数c_j两两组合,以获取L组随机变量$\{i_j,c_j\}$,其中,$1\leqslant j\leqslant L$。

[0054] 具体说明如下:在7个子文件中(m=7)中选择3(L=3)个子文件,分别记作子文件1、子文件2和子文件3;生成与子文件1对应的随机数20、与子文件2对应的随机数25、与子文件3对应的随机数15(需要说明的是:随机数的取值范围可以在预设的有限域之内,预设的有限域的范围可以根据实际情况自主设置,例如1～255);获取3组随机变量为{子文件1,20}、{子文件2,25}、{子文件3,15}。

[0055] 向云服务器发送数据查询请求，所述数据查询请求携带有所述L组随机变量，以供所述云服务器根据预先存储的文件分割后子文件的标签、所述数据查询请求和第二预设规则，获取反映待检测文件完整性的计算结果；其中，1≤L≤m。

[0056] 具体的，终端向云服务器发送数据查询请求，所述数据查询请求携带有所述L组随机变量，以供所述云服务器根据预先存储的文件分割后子文件的标签、所述数据查询请求和第二预设规则，获取反映待检测文件完整性的计算结果；其中，1≤L≤m。数据查询请求可以理解为待检测文件的数据完整性的查询请求。对于云服务器根据预先存储的文件分割后子文件的标签、所述数据查询请求和第二预设规则，获取反映待检测文件完整性的计算结果的详细说明，可参照后续云服务器作为执行主体的验证待检测文件完整性的方法介绍。

[0057] 接收所述云服务器返回的所述计算结果，并根据所述计算结果、所述L组随机变量、所述标识、预先获得的秘钥和第三预设规则，验证所述待检测文件完整性。

[0058] 具体的，终端接收所述云服务器返回的所述计算结果，并根据所述计算结果、所述L组随机变量、所述标识、预先获得的秘钥和第三预设规则，验证所述待检测文件完整性。计算结果(w,t)中的第一子文件向量w和所述第二子文件向量t的获取步骤可以参照后续云服务器作为执行主体的验证待检测文件完整性的方法介绍。对于根据所述计算结果、所述L组随机变量、所述标识、预先获得的秘钥和第三预设规则，验证所述待检测文件完整性详细说明如下：

[0059] 预先获得的秘钥可以包括第一秘钥K1和第二秘钥K2，将第一秘钥K1输入第一预设函数(可以是IEEE Std 1363-2000标准中的密钥导出函数KDF1)，将该KDF1的输出值作为向量u；

[0060] 将向量u与计算结果中的第一子文件向量w进行内积运算，以获取内积运算结果a，第一子文件向量w的获取可参照后续云服务器作为执行主体的验证待检测文件完整性的方法介绍。

[0061] 将第二秘钥K2、待检测文件的标识和L组随机变量中的子文件标识i_j输入第二预设函数(可以是伪随机函数)，以获取中间计算结果H(K2,(id,i_j))；

[0062] 再根据如下公式获取中间参数b：

[0063] $$b=\sum_{j=1}^{L}c_j\cdot[H(K2,(id,i_j))];$$

[0064] 其中，c_j为L组随机变量中的随机数、H为第二预设函数、K2为第二秘钥；

[0065] 再将内积运算结果a与中间参数b相加，如果a+b等于计算结果中的第二子文件向量t，则验证待检测文件完整性为完整；如果a+b不等于计算结果中的第二子文件向量t，则验证待检测文件完整性为不完整。

[0066] 本发明实施例提供的基于云存储的区块链可靠数据存储方法，通过将待检测文件存储在云服务器，并验证由云服务器返回的计算结果，能够对待检测文件完整性进行准确验证。

[0067] 在上述实施例的基础上，所述根据所述子文件数m和第一预设规则，生成L组随机变量，包括：

[0068] 在所述子文件m中选择L个子文件。

[0069] 具体的，终端在所述子文件m中选择L个子文件。可参照上述实施例，不再赘述。

[0070] 生成与每一个子文件标识i_j一一对应的随机数c_j,所述随机数的取值范围在预设的有限域之内。

[0071] 具体的,终端生成与每一个子文件标识i_j一一对应的随机数c_j,所述随机数的取值范围在预设的有限域之内。可参照上述实施例,不再赘述。

[0072] 将所述子文件标识i_j和所述随机数c_j两两组合,以获取L组随机变量$\{i_j,c_j\}$,其中,$1\leqslant j\leqslant L$。

[0073] 具体的,终端将所述子文件标识i_j和所述随机数c_j两两组合,以获取L组随机变量$\{i_j,c_j\}$,其中,$1\leqslant j\leqslant L$。可参照上述实施例,不再赘述。

[0074] 本发明实施例提供的基于云存储的区块链可靠数据存储方法,通过生成L组随机变量,保证了对待检测文件完整性进行验证的顺利进行。

[0075] 在上述实施例的基础上,预先获得的秘钥包括第一秘钥K1和第二秘钥K2,相应的;所述根据所述计算结果、所述L组随机变量、所述标识、预先获得的秘钥和第三预设规则,验证所述待检测文件完整性,包括:

[0076] 将所述第一秘钥K1输入第一预设函数,以获取向量元素数为n的向量u。

[0077] 具体的,终端将所述第一秘钥K1输入第一预设函数,以获取向量元素数为n的向量u。可参照上述实施例,不再赘述。

[0078] 将所述向量u与所述计算结果中的第一子文件向量w进行内积运算,以获取内积运算结果a。

[0079] 具体的,终端将所述向量u与所述计算结果中的第一子文件向量w进行内积运算,以获取内积运算结果a。可参照上述实施例,不再赘述。

[0080] 将所述第二秘钥K2、所述标识和所述L组随机变量中的子文件标识i_j输入第二预设函数,以获取中间计算结果$H(K2,(id,i_j))$,其中,id为所述标识,i_j为子文件标识。

[0081] 具体的,终端将所述第二秘钥K2、所述标识和所述L组随机变量中的子文件标识i_j输入第二预设函数,以获取中间计算结果$H(K2,(id,i_j))$,其中,id为所述标识,i_j为子文件标识。可参照上述实施例,不再赘述。

[0082] 根据所述中间计算结果$H(K2,(id,i_j))$和所述L组随机变量中的随机数c_j获取中间参数b。

[0083] 具体的,终端根据所述中间计算结果$H(K2,(id,i_j))$和所述L组随机变量中的随机数c_j获取中间参数b。可参照上述实施例,不再赘述。

[0084] 根据所述内积运算结果a、所述中间参数b和所述计算结果中的第二子文件向量t,验证所述待检测文件完整性。

[0085] 具体的,终端根据所述内积运算结果a、所述中间参数b和所述计算结果中的第二子文件向量t,验证所述待检测文件完整性。可参照上述实施例,不再赘述。

[0086] 本发明实施例提供的基于云存储的区块链可靠数据存储方法,通过预先获得的秘钥计算验证待检测文件过程中的参数,还能够保证存储在云服务器中的文件数据的安全。

[0087] 在上述实施例的基础上,根据所述中间计算结果$H(K2,(id,i_j))$和所述L组随机变量中的随机数c_j获取中间参数b,包括:

[0088] 根据如下公式获取中间参数b:

[0089] $$b=\sum_{j=1}^{L}c_j\cdot[H(K2,(id,i_j))];$$

[0090] 其中，c_j为L组随机变量中的随机数、H为第二预设函数、K2为第二秘钥、id为所述标识、i_j为子文件标识、$1\leqslant j\leqslant L$。

[0091] 具体的，终端根据如下公式获取中间参数b：

[0092] $$b=\sum_{j=1}^{L}c_j\cdot[H(K2,(id,i_j))];$$

[0093] 其中，c_j为L组随机变量中的随机数、H为第二预设函数、K2为第二秘钥、id为所述标识、i_j为为子文件标识、$1\leqslant j\leqslant L$。可参照上述实施例，不再赘述。

[0094] 本发明实施例提供的基于云存储的区块链可靠数据存储方法，通过具体的公式计算中间参数b，进一步保证了能够对待检测文件完整性进行准确验证。

[0095] 在上述实施例的基础上，所述根据所述内积运算结果a、所述中间参数b和所述第二子文件向量t，验证所述待检测文件完整性，包括：

[0096] 将内积运算结果a和中间参数b进行相加。

[0097] 具体的，终端将内积运算结果a和中间参数b进行相加。可参照上述实施例，不再赘述。

[0098] 若相加结果等于所述第二子文件向量t，则验证所述待检测文件完整性为完整。

[0099] 具体的，终端若判断获知相加结果等于所述第二子文件向量t，则验证所述待检测文件完整性为完整。可参照上述实施例，不再赘述。

[0100] 或，

[0101] 若相加结果不等于所述第二子文件向量t，则验证所述待检测文件完整性为不完整。

[0102] 具体的，终端若判断获知相加结果不等于所述第二子文件向量t，则验证所述待检测文件完整性为不完整。可参照上述实施例，不再赘述。

[0103] 本发明实施例提供的基于云存储的区块链可靠数据存储方法，通过验证a和b相加结果是否等于第二子文件向量t，能够准确地对待检测文件完整性进行验证。

[0104] 在上述实施例的基础上，在获取待检测文件被分割的子文件数m和所述待检测文件的标识的步骤之前，所述方法还包括：

[0105] 分别指定所有文件中的每一个文件的标识。

[0106] 具体的，终端分别指定所有文件中的每一个文件的标识。即终端为每一个文件指定一个id，以区分不同的文件。

[0107] 将所述每一个文件平均分成m份，并进行向量化，以获取向量集合vi。

[0108] 具体的，终端将所述每一个文件平均分成m份，并进行向量化，以获取向量集合vi。向量化后的集合为$\{v_i=[v_{i1}....v_{in}]\}_{i=1...m}$，n可选为1024，举例说明如下：1个大小为6KB的文件，参照上述举例$m=6$，每一块对应的向量分别为$\{v_1=[v_{11}....v_{1n}]\}\cdots\{v_m=[v_{m1}....v_{mn}]\}$；即$v_1..v_m$分别对应1KB的大小。

[0109] 将随机生成的第一秘钥K1输入第一预设函数，以获取向量元素数为n的向量u。

[0110] 具体的，终端将随机生成的第一秘钥K1输入第一预设函数，以获取向量元素数为n的向量u。可参照上述举例。

[0111] 将随机生成的第二秘钥K2、所述每一个文件的标识和m个子文件中的每一个子文件i输入第二预设函数H,以获取m个计算值b_i。

[0112] 具体的,终端将随机生成的第二秘钥K2、所述每一个文件的标识和m个子文件中的每一个子文件i输入第二预设函数H,以获取m个计算值b_i。需要说明的是:i可以理解为每一个子文件标识,通过文件标识和子文件标识的结合可以确定哪一个文件中的哪一个子文件。获取m个计算值b_i可参照上述举例。

[0113] 将向量u和所述向量集合vi进行内积运算,以获取m个计算结果。

[0114] 具体的,终端将向量u和所述向量集合vi进行内积运算,以获取m个计算结果。对于内积运算不再作具体说明。

[0115] 将m个计算结果中的每一个与每一个计算值b_i分别相加,相加的结果作为ti。

[0116] 具体的,终端将m个计算结果中的每一个与每一个计算值b_i分别相加,相加的结果作为ti。可以计算出m个ti。

[0117] 将结果(vi,ti)和所述每一个文件的标识作为子文件的标签,并发送至云服务器,以供所述云服务器根据所述子文件的标签,获取待检测文件中的子文件信息(vi_j,ti_j)。

[0118] 具体的,终端将结果(vi,ti)和所述每一个文件的标识作为子文件的标签,并发送至云服务器,以供所述云服务器根据所述子文件的标签,获取待检测文件中的子文件信息(vi_j,ti_j)。云服务器根据所述子文件的标签,获取待检测文件中的子文件信息(vi_j,ti_j)的详细说明,可参照后续云服务器作为执行主体的验证待检测文件完整性的方法介绍。

[0119] 本发明实施例提供的基于云存储的区块链可靠数据存储方法,通过合理地对文件进行分割、以及对子文件的标签,能够使得云服务器更加合理地获取待检测文件中的子文件信息,从而在终端能够准确检验出待检测文件是否完整。

[0120] 图3为本发明另一实施例基于云存储的区块链可靠数据存储方法流程示意图,如图3所示:对一种基于云存储的区块链可靠数据存储方法做进一步说明:(执行主体为云服务器)

[0121] S10:接收终端发送的数据查询请求,所述数据查询请求携带有L组随机变量。

[0122] 具体的,云服务器接收终端发送的数据查询请求,所述数据查询请求携带有L组随机变量。数据查询请求可以理解为待检测文件的数据完整性的查询请求。L组随机变量获取的步骤可参照上述实施例。

[0123] S20:根据预先存储的子文件的标签、所述数据查询请求和第二预设规则,获取反映待检测文件完整性的计算结果。

[0124] 具体的,云服务器根据预先存储的子文件的标签、所述数据查询请求和第二预设规则,获取反映待检测文件完整性的计算结果。详细说明如下:

[0125] 根据预先存储的子文件的标签(包括(vi,ti)和文件的标识)、数据查询请求和第二预设规则,获取与数据查询请求对应的待检测文件中的子文件信息(vi_j,ti_j);参照上述举例:待检测文件被分成7个子文件(m=7),需要对其中的3个子文件进行检测(L=3),则j的取值为1、2、3。

[0126] 根据如下公式分别计算第一子文件向量w和第二子文件向量t:

[0127] $$w=\sum_{j=1}^{L}c_j\cdot vi_j$$

[0128] 其中，w为第一子文件向量、c_j为L组随机变量中的随机数、vi_j为所述子文件信息的第一分量。参照上述举例，w＝20*待检测子文件对应的向量vi_1+25*待检测子文件对应的向量vi_2+15*待检测子文件对应的向量vi_3

[0129] $$t=\sum_{j=1}^{L}c_j\cdot ti_j$$

[0130] 其中，t为第二子文件向量、c_j为L组随机变量中的随机数、ti_j为子文件信息的第二分量；可参照上述计算w的步骤，不再赘述。

[0131] 将所述第一子文件向量w和所述第二子文件向量t组合，以获取所述计算结果(w，t)。

[0132] S30：将所述计算结果发送至所述终端，以供所述终端根据所述计算结果、所述L组随机变量、待检测文件的标识、预先获得的秘钥和第三预设规则，验证所述待检测文件完整性。

[0133] 具体的，云服务器将所述计算结果发送至所述终端，以供所述终端根据所述计算结果、所述L组随机变量、待检测文件的标识、预先获得的秘钥和第三预设规则，验证所述待检测文件完整性。终端根据所述计算结果、所述L组随机变量、待检测文件的标识、预先获得的秘钥和第三预设规则，验证所述待检测文件完整性的介绍可参照上述实施例，不再赘述。

[0134] 本发明实施例提供的基于云存储的区块链可靠数据存储方法，通过合理地计算出的第一子文件向量w和第二子文件向量t，并发送给终端，使得终端能够准确验证待检测文件的完整性。

[0135] 在上述实施例的基础上，所述根据预先存储的子文件的标签、所述数据查询请求和第二预设规则，获取反映待检测文件完整性的计算结果，包括：

[0136] 根据预先存储的子文件的标签、所述数据查询请求和第二预设规则，获取与所述数据查询请求对应的待检测文件中的子文件信息(vi_j,ti_j)。

[0137] 具体的，云服务器根据预先存储的子文件的标签、所述数据查询请求和第二预设规则，获取与所述数据查询请求对应的待检测文件中的子文件信息(vi_j,ti_j)；可参照上述实施例，不再赘述。

[0138] 根据如下公式分别计算第一子文件向量w和第二子文件向量t：

[0139] $$w=\sum_{j=1}^{L}c_j\cdot vi_j$$

[0140] 其中，w为第一子文件向量、c_j为L组随机变量中的随机数、vi_j为所述子文件信息的第一分量。

[0141] $$t=\sum_{j=1}^{L}c_j\cdot ti_j$$

[0142] 其中，t为第二子文件向量、c_j为L组随机变量中的随机数、ti_j为所述子文件信息的第二分量。

[0143] 具体的，云服务器根据如下公式分别计算第一子文件向量w和第二子文件向量t：

[0144] $$w=\sum_{j=1}^{L}c_j\cdot vi_j$$

[0145] 其中，w为第一子文件向量、c_j为L组随机变量中的随机数、vi_j为所述子文件信息的第一分量；可参照上述实施例，不再赘述。

[0146] $$t=\sum_{j=1}^{L}c_j\cdot ti_j$$

[0147] 其中，t为第二子文件向量、c_j为L组随机变量中的随机数、ti_j为所述子文件信息的第二分量；可参照上述实施例，不再赘述。

[0148] 将所述第一子文件向量w和所述第二子文件向量t组合，以获取所述计算结果(w,t)。

[0149] 具体的，云服务器将所述第一子文件向量w和所述第二子文件向量t组合，以获取所述计算结果(w,t)。可参照上述实施例，不再赘述。

[0150] 本发明实施例提供的基于云存储的区块链可靠数据存储方法，能够更加合理地计算出的第一子文件向量w和第二子文件向量t，并发送给终端，使得终端进一步能够准确验证待检测文件的完整性。

[0151] 下面对本发明实施例基于云存储的区块链可靠数据存储方法的步骤进一步说明如下：参照图2实现基于云存储的区块链架构被划分为两个部分，内部网络(本地存储)及云(云存储)。内部网络由多个节点以P2P网络相互连接，共同参与新的交易数据及区块的产生，并将区块封装的一段时间内产生的所有交易数据外包存储至云端(云服务器)，通过与云服务器的交互可以验证数据存储的完整性和/或下载指定的交易数据。

[0152] 区块链是由一系列具有时间先后顺序的且具有特定结构的数据区块按区块哈希值链接组成，每个区块中记录着在一段时间内产生的所有交易数据。本发明实施例将数据本身外包存储，而为了描述数据产生顺序以及保证数据不被篡改等结构化数据则在每个节点处均有备份。这样做的目的是为了使区块链系统的正常运行无需频繁地与云服务器交互，以此保证运行效率。因此，在云端和节点本地均各自存储数据，但节点本地存储的数据仅占很小的存储空间。相应的数据结构如图2所示，存储于节点本地的结构化数据，是由一些列具有特殊结构的区块链接组成，以创世区块作为开端。除创世区块外，每个区块均包含区块序列号、区块头、区块大小、区块哈希及数据对应表字段。区块头记录父区块哈希、时间戳、Merkle根。其中，Merkle根是将该区块封装的所有交易数据构成的Merkle哈希树的根节点的值。不用下载所有的数据即可利用Merkle树结构快速地验证该区块存在某个特定的数据。存储于云端的数据与节点本地存储的数据结构一一对应，以区块作为存储的基本单元。为了实现可靠存储，需要采用安全云存储机制。因此，存储于云端的数据被按照特定的格式分割并标签化。分割之后的数据与真实的数据存在对应关系，该关系被记录在数据对应表中，被存储于节点本地，而数据被存储于云服务器，利用该数据对应表，每个节点都可以快速地定位数据，减少搜索时间，提高下载速率。

[0153] 图4为本发明实施例基于云存储的区块链可靠数据存储系统流程图，首先生成创世区块，之后所有节点共同参与新区块的持续生成，包括：当任意节点产生新数据之后，将该数据广播至全网，当未达到产生新区块的触发条件时(如时间片未结束、数据量不够等)，则重复以上步骤；当新区块产生时，则利用选取的安全云存储机制的相应算法(对应于上述的第一、第二、第三预设规则)处理该新区块包含的所有数据，即分割数据并标签化，并生成相应的数据对应表及结构化数据并将其共享至全网内所有节点，将处理过后的数据外包存

储至云端;当一个区块处理完毕之后,则进入下一个区块的轮次,即重复以上的所有步骤。在区块不断增多的过程中,存在以下两种事件:当需要检验存储有效性时,则生成验证请求,等待云服务器返回的证据,验证该证据的正确性,若验证失败,则说明云端存在数据丢失。当需要下载数据时,则根据区块序列号、数据对应表等生成下载请求,等待云服务器的响应,处理返回的内容获取需要的原始数据。需要说明的是:图4中的“检验存储有效性”和“下载数据”的步骤并无时序上的先后关系,是根据终端发送的相应请求进行触发的。

[0154] 图5为本发明实施例基于云存储的区块链可靠数据存储终端结构示意图,如图5所示,本发明实施例提供了一种基于云存储的区块链可靠数据存储终端,所述终端包括获取单元51、标识单元52、建立单元53和存储单元54,其中:

[0155] 获取单元51用于按区块为单位获取区块链中的文件;标识单元52用于对区块链中的文件进行分割,并标识分割后的文件;建立单元53用于建立标识后的子文件与Merkle哈希树结构除根节点外所有子节点之间的映射关系;存储单元54用于将标识后的文件存储于云服务器,并根据所述映射关系从所述云服务器中获取所述标识后的文件。

[0156] 具体的,获取单元51用于按区块为单位获取区块链中的文件;标识单元52用于对区块链中的文件进行分割,并标识分割后的文件;建立单元53用于建立标识后的子文件与Merkle哈希树结构除根节点外所有子节点之间的映射关系;存储单元54用于将标识后的文件存储于云服务器,并根据所述映射关系从所述云服务器中获取所述标识后的文件。

[0157] 本发明实施例提供的基于云存储的区块链可靠数据存储终端,将数据外包存储至云服务器,终端可周期性地审计数据的完整性。

[0158] 所述终端还可以包括下载单元55,用于在指定需要下载的数据后根据所述映射关系从所述云服务器中获取相应的标识后的文件,并进行下载到本地;验证单元56,用于对存储于云服务器上的标识后的文件进行文件完整性的验证。

[0159] 本发明实施例提供的基于云存储的区块链可靠数据存储终端具体可以用于执行上述各方法实施例的处理流程,其功能在此不再赘述,可以参照上述方法实施例的详细描述。

[0160] 图6为本发明实施例基于云存储的区块链可靠数据存储系统结构示意图,如图6所示,本发明实施例提供一种基于云存储的区块链可靠数据存储系统,所述系统包括终端1和云服务器2。

[0161] 图7为本发明实施例提供的终端实体结构示意图,如图7所示,所述终端包括:处理器(processor)701、存储器(memory)702和总线703;

[0162] 其中,所述处理器701、存储器702通过总线703完成相互间的通信;

[0163] 所述处理器701用于调用所述存储器702中的程序指令,以执行上述各方法实施例所提供的方法,例如包括:按区块为单位获取区块链中的文件;对区块链中的文件进行分割,并标识分割后的文件;建立标识后的子文件与Merkle哈希树结构除根节点外所有子节点之间的映射关系;将标识后的文件存储于云服务器,并根据所述映射关系从所述云服务器中获取所述标识后的文件。

[0164] 本实施例公开一种计算机程序产品,所述计算机程序产品包括存储在非暂态计算机可读存储介质上的计算机程序,所述计算机程序包括程序指令,当所述程序指令被计算机执行时,计算机能够执行上述各方法实施例所提供的方法,例如包括:按区块为单位获取

区块链中的文件;对区块链中的文件进行分割,并标识分割后的文件;建立标识后的子文件与Merkle哈希树结构除根节点外所有子节点之间的映射关系;将标识后的文件存储于云服务器,并根据所述映射关系从所述云服务器中获取所述标识后的文件。

[0165] 本实施例提供一种非暂态计算机可读存储介质,所述非暂态计算机可读存储介质存储计算机指令,所述计算机指令使所述计算机执行上述各方法实施例所提供的方法,例如包括按区块为单位获取区块链中的文件;对区块链中的文件进行分割,并标识分割后的文件;建立标识后的子文件与Merkle哈希树结构除根节点外所有子节点之间的映射关系;将标识后的文件存储于云服务器,并根据所述映射关系从所述云服务器中获取所述标识后的文件。

[0166] 本领域普通技术人员可以理解:实现上述方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成,前述的程序可以存储于一计算机可读取存储介质中,该程序在执行时,执行包括上述方法实施例的步骤;而前述的存储介质包括:ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

[0167] 以上所描述的终端等实施例仅仅是示意性的,其中所述作为分离部件说明的单元可以是或者也可以不是物理上分开的,作为单元显示的部件可以是或者也可以不是物理单元,即可以位于一个地方,或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本实施例方案的目的。本领域普通技术人员在不付出创造性的劳动的情况下,即可以理解并实施。

[0168] 通过以上的实施方式的描述,本领域的技术人员可以清楚地了解到各实施方式可借助软件加必需的通用硬件平台的方式来实现,当然也可以通过硬件。基于这样的理解,上述技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来,该计算机软件产品可以存储在计算机可读存储介质中,如ROM/RAM、磁碟、光盘等,包括若干指令用以使得一台计算机设备(可以是个人计算机,服务器,或者网络设备等)执行各个实施例或者实施例的某些部分所述的方法。

[0169] 最后应说明的是:以上各实施例仅用以说明本发明的实施例的技术方案,而非对其限制;尽管参照前述各实施例对本发明的实施例进行了详细的说明,本领域的普通技术人员应当理解:其依然可以对前述各实施例所记载的技术方案进行修改,或者对其中部分或者全部技术特征进行等同替换;而这些修改或者替换,并不使相应技术方案的本质脱离本发明的实施例各实施例技术方案的范围。

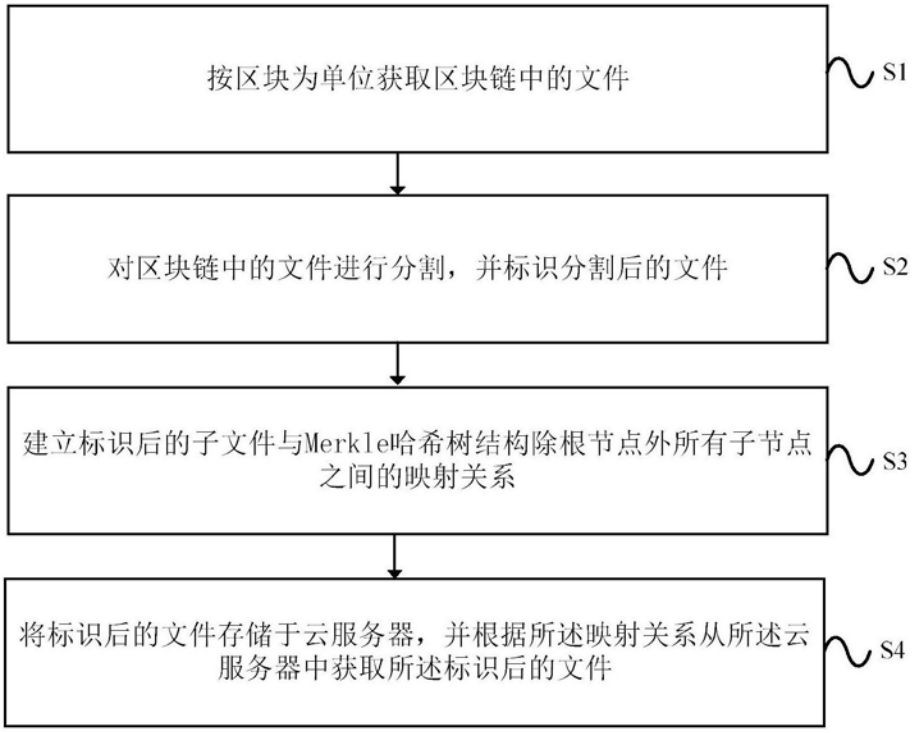

按区块为单位获取区块链中的文件
S1
对区块链中的文件进行分割，并标识分割后的文件
S2
建立标识后的子文件与Merkle哈希树结构除根节点外所有子节点之间的映射关系
S3
将标识后的文件存储于云服务器，并根据所述映射关系从所述云服务器中获取所述标识后的文件
S4

图1

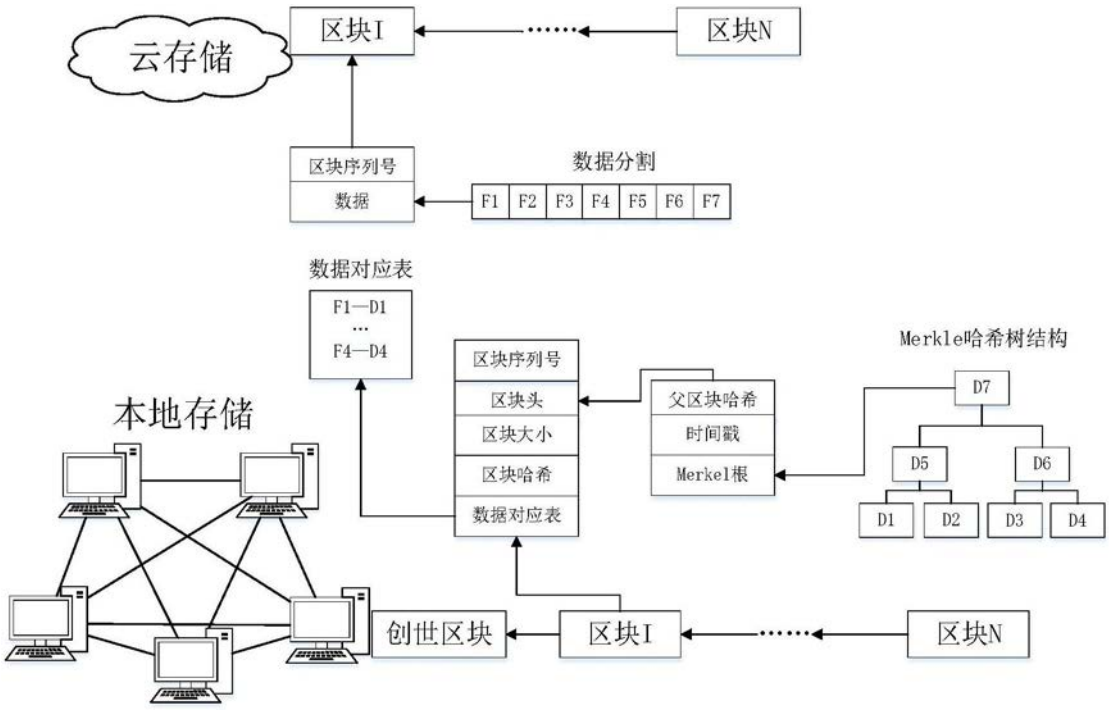

云存储
区块I
区块N
区块序列号
数据
数据分割
F1 F2 F3 F4 F5 F6 F7
数据对应表
F1—D1
…
F4—D4
本地存储
区块序列号
区块头
区块大小
区块哈希
数据对应表
父区块哈希
时间戳
Merkel根
Merkle哈希树结构
D7
D5
D6
D1
D2
D3
D4
创世区块
区块I
区块N

图2

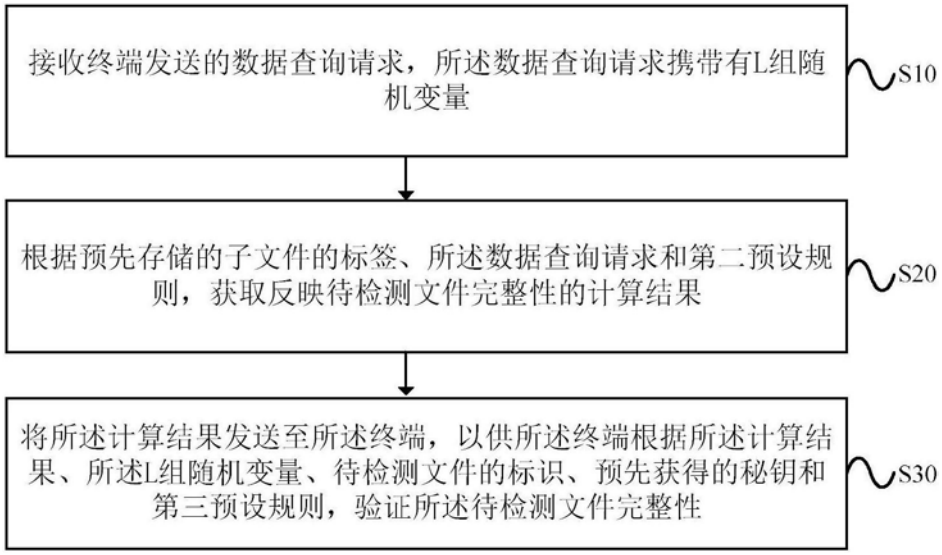

接收终端发送的数据查询请求，所述数据查询请求携带有L组随机变量
S10
根据预先存储的子文件的标签、所述数据查询请求和第二预设规则，获取反映待检测文件完整性的计算结果
S20
将所述计算结果发送至所述终端，以供所述终端根据所述计算结果、所述L组随机变量、待检测文件的标识、预先获得的秘钥和第三预设规则，验证所述待检测文件完整性
S30

图3

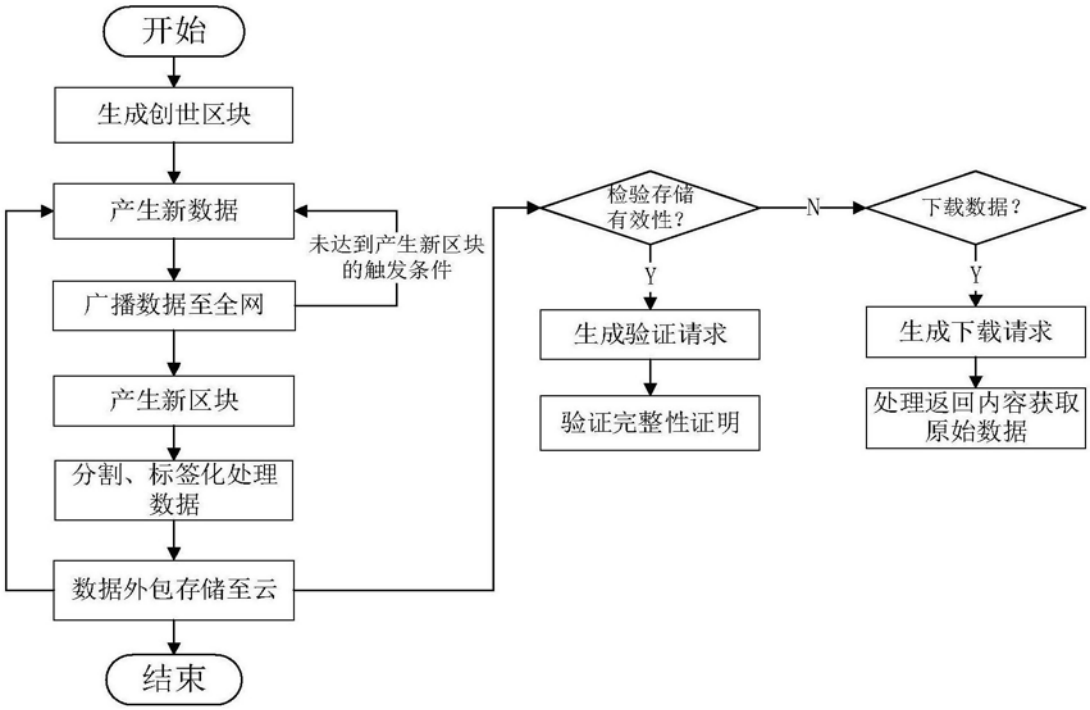

开始
生成创世区块
产生新数据
未达到产生新区块的触发条件
广播数据至全网
产生新区块
分割、标签化处理数据
数据外包存储至云
结束
检验存储有效性？
N
下载数据？
Y
Y
生成验证请求
验证完整性证明
生成下载请求
处理返回内容获取原始数据

图4

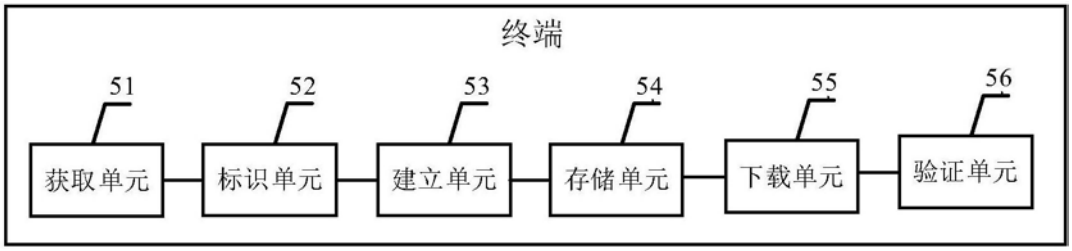

终端
51
52
53
54
55
56
获取单元
标识单元
建立单元
存储单元
下载单元
验证单元

图5

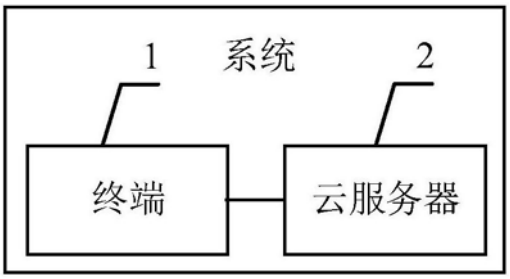

1
系统
2
终端
云服务器

图6

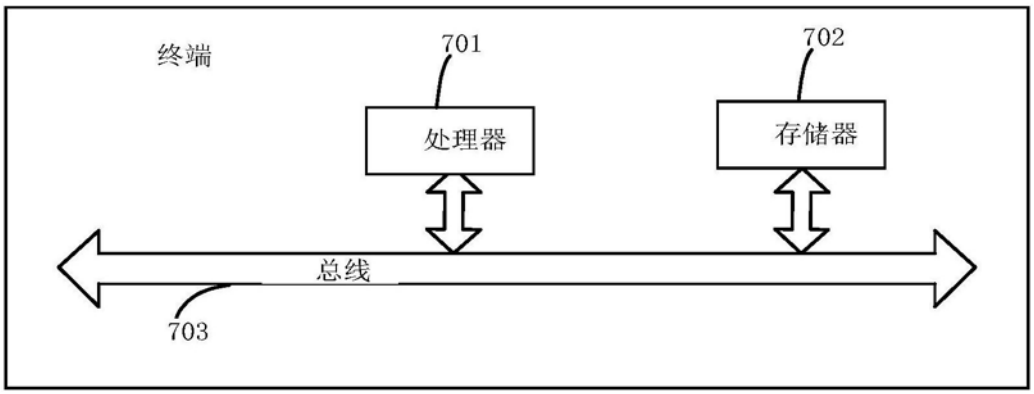

终端
701
702
处理器
存储器
总线
703

图7