(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2020 年 7 月 30 日 (30.07.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/151330 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2019/118146

(22) 国际申请日: 2019 年 11 月 13 日 (13.11.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910063626.X 2019年1月23日 (23.01.2019) CN

(71) 申请人: 平安科技（深圳）有限公司 (PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) [CN/CN]; 中国广东省深圳市福田区福田街道福安社区益田路5033号平安金融中心23楼, Guangdong 518000 (CN)。

(72) 发明人: 梁劲峰 (LIANG, Jinfeng); 中国广东省深圳市福田区福田街道福安社区益田路5033号平安金融中心23楼, Guangdong 518000 (CN)。 郑映锋 (ZHENG, Yingfeng); 中国广东省深圳市福田区福田街道福安社区益田路5033号平安金融中心23楼, Guangdong 518000 (CN)。

(74) 代理人: 深圳中一联合知识产权代理有限公司 (SHENZHEN ZHONGYI UNION INTELLECTUAL PROPERTY AGENCY CO., LTD.); 中国广东省深圳市福田区园岭街道深南中路1014号报春大厦9楼（5号信箱）, Guangdong 518028 (CN)。

(81) 指定国 (除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS,

(54) **Title:** DATA POSSESSION VERIFICATION METHOD AND TERMINAL DEVICE

(54) **发明名称**: 数据持有性验证方法及终端设备

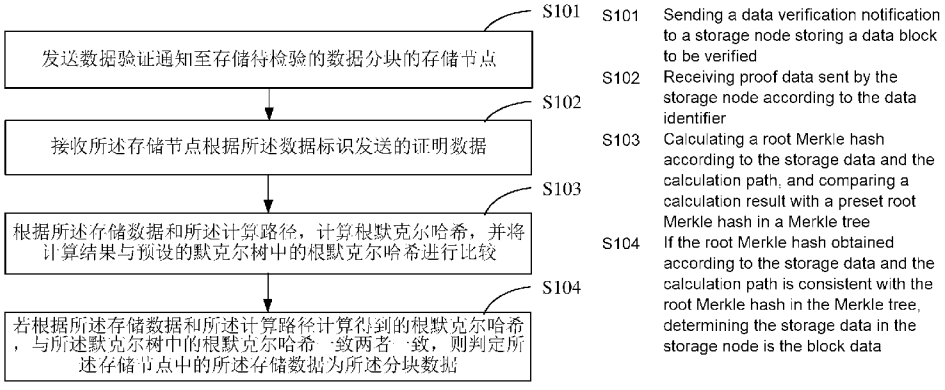

图 1

(57) **Abstract:** An embodiment of the present application is applied to the technical field of computer applications, provides a data possession verification method, a terminal device and a computer readable storage medium, comprising: dividing original data of a data owner terminal into blocks, and storing the data blocks into a corresponding storage node; after determining the storage data to be verified, calculating a root Merkle hash according to the storage data sent by the storage node and a calculation path for calculating the root Merkle hash; and comparing a calculation result with a pre-stored Merkle hash to determine the correctness of the storage data stored in the storage node, thereby ensuring the possession and integrity of the storage data of the storage node in the point-to-point storage process.

(57) **摘要**: 本申请实施例适用于计算机应用技术领域，提供了一种数据持有性验证方法、终端设备及计算机可读存储介质，包括：通过对数据所有者终端的原始数据进行分块，并将数据分块存储至对应的存储节点中，在确定了待验证的存储数据之后，根据存储节点发送的存储数据和计算根默克尔哈希的计算路径，计算根默克尔哈希，将计算结果与预先存储的根默克尔哈希进行对比，以确定存储节点所存储的存储数据的正确性，保证了点对点存储过程中存储节点保存数据的持有性和完整性。

WO 2020/151330 A1

[见续页]

JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

数据持有性验证方法及终端设备

[0001] 本申请申明享有2019年01月23日递交的申请号为201910063626.X、名称为“数据持有性验证方法及终端设备”中国专利申请的优先权，该中国专利申请的整体内容以参考的方式结合在本申请中。

技术领域

[0002] 本申请属于计算机应用技术领域，特别是涉及一种数据持有性验证方法及终端设备。

背景技术

[0003] 云用户利用云服务器提供的存储服务将本地数据存储在云端，不仅可以节省本地的存储空间和计算资源，还可以实现与其他用户的资源共享。在复杂的云计算环境下，受到人为因素的影响，云服务器可能非故意的删除数据或者修改数据。在对等网络（Peer to Peer，P2P）分布式云存储系统中，由于无法保证节点的可信性，有些节点可能声称存储了其并没有存储的数据，以换取更多的经济收益。因此数据所有者，或其委托的检查者，需要定期对声称存储了该数据的存储节发起数据持有性检查，以判断存储节点是否完好地保存了用户的数据。

[0004] 现有技术中通过对存储节点所存储的数据与原始数据进行对比，来确定存储节点中的数据是否被修改或者删除，但是当数据量较大的情况下，现有的验证方式计算的次数和消耗时间较多，验证效率较低。

发明概述

技术问题

[0005] 有鉴于此，本申请实施例提供了一种数据持有性验证方法及终端设备，以解决当数据量较大的情况下，现有的验证方式计算的次数和消耗时间较多，验证效率较低的问题。

问题的解决方案

技术解决方案

[0006] 为解决上述技术问题，本申请实施例采用的技术方案是：

[0007] 第一方面，提供了一种数据持有性验证方法，包括：

[0008] 发送数据验证通知至存储待检验的数据分块的存储节点；所述数据验证通知包括所述待检验的数据分块的数据标识；

[0009] 接收所述存储节点根据所述数据标识发送的证明数据；所述证明数据包括所述存储节点中与所述数据标识对应的存储数据，以及根据所述存储数据计算根默克尔哈希的计算路径；

[0010] 根据所述存储数据和所述计算路径，计算根默克尔哈希，并将计算结果与预设的默克尔树中的根默克尔哈希进行比较；

[0011] 若根据所述存储数据和所述计算路径计算得到的根默克尔哈希，与所述默克尔树中的根默克尔哈希一致，则判定所述存储节点中的所述存储数据为所述分块数据。

[0012] 第二方面，提供了一种终端设备，包括存储器、处理器以及存储在所述存储器中并可在所述处理器上运行的计算机可读指令，所述处理器执行所述计算机可读指令时实现上述数据持有性验证方法的如下步骤：

[0013] 发送数据验证通知至存储待检验的数据分块的存储节点；所述数据验证通知包括所述待检验的数据分块的数据标识；

[0014] 接收所述存储节点根据所述数据标识发送的证明数据；所述证明数据包括所述存储节点中与所述数据标识对应的存储数据，以及根据所述存储数据计算根默克尔哈希的计算路径；

[0015] 根据所述存储数据和所述计算路径，计算根默克尔哈希，并将计算结果与预设的默克尔树中的根默克尔哈希进行比较；

[0016] 若根据所述存储数据和所述计算路径计算得到的根默克尔哈希，与所述默克尔树中的根默克尔哈希一致，则判定所述存储节点中的所述存储数据为所述分块数据。

[0017] 第三方面，提供了一种终端设备，包括：

[0018] 发送单元，用于发送数据验证通知至存储待检验的数据分块的存储节点；所述数据验证通知包括所述待检验的数据分块的数据标识；

[0019] 接收单元，用于接收所述存储节点根据所述数据标识发送的证明数据；所述证

明数据包括所述存储节点中与所述数据标识对应的存储数据，以及根据所述存储数据计算根默克尔哈希的计算路径；

[0020] 计算单元，用于根据所述存储数据和所述计算路径，计算根默克尔哈希，并将计算结果与预设的默克尔树中的根默克尔哈希进行比较；

[0021] 判定单元，用于若根据所述存储数据和所述计算路径计算得到的根默克尔哈希，与所述默克尔树中的根默克尔哈希一致，则判定所述存储节点中的所述存储数据为所述分块数据。

[0022] 第四方面，提供了一种计算机非易失性可读存储介质，所述计算机非易失性可读存储介质存储有计算机可读指令，所述计算机可读指令被处理器执行时实现上述数据持有性验证方法的如下步骤：

[0023] 发送数据验证通知至存储待检验的数据分块的存储节点；所述数据验证通知包括所述待检验的数据分块的数据标识；

[0024] 接收所述存储节点根据所述数据标识发送的证明数据；所述证明数据包括所述存储节点中与所述数据标识对应的存储数据，以及根据所述存储数据计算根默克尔哈希的计算路径；

[0025] 根据所述存储数据和所述计算路径，计算根默克尔哈希，并将计算结果与预设的默克尔树中的根默克尔哈希进行比较；

[0026] 若根据所述存储数据和所述计算路径计算得到的根默克尔哈希，与所述默克尔树中的根默克尔哈希一致，则判定所述存储节点中的所述存储数据为所述分块数据。

[0027] 本申请实施例提供的数据持有性验证方法及终端设备的有益效果在于：通过对数据所有者终端的原始数据进行分块，并将数据分块存储至对应的存储节点中，在确定了待验证的存储数据之后，根据存储节点发送的存储数据和计算根默克尔哈希的计算路径，计算根默克尔哈希，将计算结果与预先存储的根默克尔哈希进行对比，以确定存储节点所存储的存储数据的正确性，保证了点对点存储过程中存储节点保存数据的持有性和完整性。

发明的有益效果

对附图的简要说明

附图说明

[0028] 图1是本申请实施例一提供的数据持有性验证方法的流程图；

[0029] 图2是本申请实施例二提供的数据持有性验证方法的流程图；

[0030] 图3是本申请实施例三提供的终端设备的示意图；

[0031] 图4是本申请实施例四提供的终端设备的示意图。

发明实施例

本发明的实施方式

[0032] 参见图1，图1是本申请实施例一提供的数据持有性验证方法的流程图。本实施例中数据持有性验证方法的执行主体为终端。终端包括但不限于智能手机、平板电脑、可穿戴设备等移动终端，还可以是台式电脑等。如图所示的数据持有性验证方法可以包括以下步骤：

[0033] S101：发送数据验证通知至存储待检验的数据分块的存储节点；所述数据验证通知包括所述待检验的数据分块的数据标识。

[0034] 随着网格计算、物联网以及云计算等技术的快速兴起，数据正在以前所未有的速度进行增长和累积，面对如此大规模的数据，如何进行海量数据的存储和处理给存储系统带来新的挑战。在分布式存储系统发展的基础上，云存储以其低成本、高效率、良好扩展性和高可靠性等特点，迅速成为海量数据存储研究关注的热点。

[0035] 云存储是继云计算之后兴起的一种互联网技术，它通过虚拟化技术把实实在在存在的大量的物理存储设备连接到一起，它们为了实现存储服务而协同运行，最终实现向用户提供存储服务的目的。当云计算系统因需处理海量数据而具备了雄厚的存储能力之后，它就俨然已经转换成了云存储系统。用户利用云存储系统可以在任意时间的地点在云上存取数据，方便而又快捷。

[0036] 传统的单云存储仅仅依赖于一个云存储服务提供商，为了避免厂商锁定问题和提高可用性，多云存储的概念问世并吸引了越来越多的目光和关注。多云存储是同时使用多个云服务，用户的数据被按照一定的分布策略冗余的存储在多个云上。由于不同的云存储服务提供商都有其各自的特点和优势，所有多云存储可以利用不同的云服务基础设施来满足用户需求的多样性。多云存储不仅可以

避免厂商锁定问题，还可以减少由于云存储组件失效引起的服务中断或数据丢失问题。所以，与传统的单云存储对比起来多云存储可以提高数据的可用性和容错性。

[0037] 数据分块是把一份完整的数据按一定的条件划分成不同的几份，由不同的服务器来存储划分之后的内容，每份内容就叫做一个片。对于外界来说，显然不希望知道数据是从哪里来，分了多少片，因为对于应用来说，需要看到的是完整的一份数据，而不希望自己的业务逻辑中掺杂了去哪里取这份数据这样与业务无关的问题。所以在分块的同时，使得数据在物理上分开存储和处理，在逻辑上还是完整的一份。本实施例中，一个完整的源文件通过分块处理之后，可能由多个数据分块组成，并且，这些数据分块被存储在不同的存储节点中，以降低源存储节点的负载。但是存储节点可能因为想提高存储效益而删除或者修改存储在本地的数据分块，而导致数据发生错误，不能正常的进行数据处理，这种情况下，我们通过对存储节点中的数据分块进行抽查，来验证存储节点中数据分块是否正确。

[0038] 在对数据分块进行验证时，由数据所有者终端先发送数据验证通知到存储待检验的数据分块的存储节点。在本实施例中，存储节点可以有很多个，用来存储数据所有者终端的数据，数据所有者终端的数据被划分成很多数据分块，由存储节点存储。在进行数据分块验证时，先确定待验证的数据分块以及存储该数据分块的存储节点，再向该存储节点发送数据验证通知。本实施例中的数据验证通知包括待检验的数据分块的数据标识。其中，数据标识可以是数据分块的编号等，此处不做限定。

[0039] S102：接收所述存储节点根据所述数据标识发送的证明数据；所述证明数据包括所述存储节点中与所述数据标识对应的存储数据，以及根据所述存储数据计算根默克尔哈希的计算路径。

[0040] 在将数据验证通知发送至存储待检验的数据分块的存储节点之后，存储节点接收到数据验证通知，并根据数据验证通知中的数据标识确定对应的存储数据，以及根据存储数据计算根默克尔哈希的计算路径，将这两个数据作为证明数据发送至数据所有者终端。

[0041] 在本实施例中，预设有默克尔树，通过默克尔树来存储每个数据分块的根默克尔哈希，以及每个数据分块计算根默克尔哈希的计算路径。其中，默克尔树的叶子是数据块，例如，文件或者文件的集合的哈希值，非叶节点是其对应子节点串联字符串的哈希。哈希是一个把任意长度的数据映射成固定长度数据的函数。例如，对于数据完整性校验，最简单的方法是对整个数据做哈希运算得到固定长度的哈希值，然后把得到的哈希值公布在网上，这样用户下载到数据之后，对数据再次进行哈希运算，比较运算结果和网上公布的哈希值进行比较，如果两个哈希值相等，说明下载的数据没有损坏。可以这样做是因为输入数据的稍微改变就会引起哈希运算结果的面目全非，而且根据哈希值反推原始输入数据的特征是困难的。如果从一个稳定的服务器进行下载，采用单一哈希是可取的。但如果数据源不稳定，一旦数据损坏，就需要重新下载，这种下载的效率是很低的。

[0042] 在点对点网络中作数据传输的时候，会同时从多个机器上下载数据，而且很多机器可以认为是不稳定或者不可信的。为了校验数据的完整性，更好的办法是把大的文件分割成小的数据块，例如，把分割成2K为单位的数据块。这样的好处是，如果小块数据在传输过程中损坏了，那么只要重新下载这一快数据就行了，不用重新下载整个文件。BT下载的时候，在下载到真正数据之前，我们会先下载一个哈希列表。把每个小块数据的哈希值拼到一起，然后对这个长字符串在作一次哈希运算，这样就得到哈希列表的根哈希。下载数据的时候，首先从可信的数据源得到正确的根哈希，就可以用它来校验哈希列表了，然后通过校验后的哈希列表校验数据块。

[0043] S103：根据所述存储数据和所述计算路径，计算根默克尔哈希，并将计算结果与预设的默克尔树中的根默克尔哈希进行比较。

[0044] 在本实施例中的默克尔树中预先存储有每个数据分块的根默克尔哈希，在获取到存储节点发送的存储数据和计算路径之后，根据存储数据和计算路径计算根默克尔哈希，并将计算结果与预设的默克尔树中的根默克尔哈希进行比较。

[0045] 在实际应用中，在默克尔树最底层，和哈希列表一样，我们把数据分成小的数据块，有相应地哈希和它对应。但是往上走，并不是直接去运算根哈希，而是

把相邻的两个哈希合并成一个字符串，然后运算这个字符串的哈希，这样根据每两个哈希得到了一个子哈希。进一步的，如果最底层的哈希总数是单数，那到最后必然出现一个单身哈希，这种情况就直接对它进行哈希运算，所以也能得到它的子哈希。于是往上推，依然是一样的方式，可以得到数目更少的新一级哈希，最终必然形成一棵倒挂的树，到了树根的这个位置，这一代就剩下一个根哈希了，即为默克尔根。在P2P网络下载网络之前，先从可信的源获得文件的默克尔根。一旦获得了树根，就可以从其他从不可信的源获取默克尔树。通过可信的树根来检查接受到的默克尔树。如果默克尔树是损坏的或者虚假的，就从其他源获得另一个默克尔树，直到获得一个与可信树根匹配的默克尔树。

[0046] 本实施例中的默克尔树可以直接下载并立即验证默克尔树的一个分支。因为可以将文件切分成小的数据块，这样如果有一块数据损坏，仅仅重新下载这个数据块就行了。如果文件非常大，那么默克尔树和哈希表都很到，但是默克尔树可以一次下载一个分支，然后立即验证这个分支，如果分支验证通过，就可以下载数据了，而哈希表只有下载整个哈希表才能验证。

[0047] S104：若根据所述存储数据和所述计算路径计算得到的根默克尔哈希，与所述默克尔树中的根默克尔哈希一致，则判定所述存储节点中的所述存储数据为所述分块数据。

[0048] 在将计算结果与预设的默克尔树中的根默克尔哈希进行比较时，若根据存储数据和计算路径计算得到的根默克尔哈希，与默克尔树中的根默克尔哈希一致，则判定存储节点中的存储数据为分块数据。

[0049] 若根据存储数据和计算路径计算得到的根默克尔哈希，与预设的默克尔树中的根默克尔哈希不同，则判定存储节点中的存储数据与分块数据不一致，并生成验证失败记录；发送验证失败记录和存储数据对应的分块数据至存储节点，并用分块数据替换存储节点中验证失败的存储数据。

[0050] 上述方案，通过发送数据验证通知至存储待检验的数据分块的存储节点，接收存储节点根据数据标识发送的证明数据；证明数据包括存储节点中与数据标识对应的存储数据，以及根据存储数据计算根默克尔哈希的计算路径；根据存储数据和计算路径计算根默克尔哈希，并将计算结果与预设的默克尔树中的根默

克尔哈希进行比较；若根据存储数据和计算路径计算得到的根默克尔哈希，与默克尔树中的根默克尔哈希一致，则判定存储节点中的存储数据为分块数据。根据数据分块对应的存储数据以及数据分块在预存的默克尔树中的计算路径，判断数据分块在目标节点中是否存储正确，保证了点对点存储过程中存储节点保存数据的持有性和正确性。

[0051] 参见图2，图2是本申请实施例二提供的数据持有性验证方法的流程图。本实施例中数据持有性验证方法的执行主体为终端。终端包括但不限于智能手机、平板电脑、可穿戴设备等移动终端，还可以是台式电脑等。如图所示的数据持有性验证方法可以包括以下步骤:

[0052] S201：对数据所有者终端的原始数据进行分块，得到至少两个数据分块，并将每个所述数据分块发送至网络中对应的存储节点进行存储。

[0053] 本实施例中的原始数据用于表示未分块之前的一个大文件，由于这个文件较大，而带来了较大的数据处理、存储以及传输压力，因此我们通过分块的方式，将其存储在不同的存储节点中。

[0054] 对于传统的分布式系统，无非是在不同的区域搭建一些服务器，然后再在这些服务器上存储数据。它解决了一些集中式存储的问题，但是也存在着比如服务器成为瓶颈、由于带宽而带来的访问不便等问题。因此，P2P分布式存储应运而生。P2P分布式存储就是让客户也成为服务器，当在存储数据的同时，也提供空间让别人来存储。这就很好的解决了由于服务器很少而产生的瓶颈，也能在速度上加以改进。但是同样它也带来了很多的问题，例如数据稳定性、一致性、安全性、隐私性以及防攻击性都会受到或多或少的影响。本实施例主要针对的是数据的完整性问题，因为在很多情况下，我们将数据量较大的数据存储至P2P节点中，节点并不能保证数据的安全性、私密性和完整性，而完整性相比于私密性是更加重要的数据属性，如果完整性收到威胁，则我们的数据处理系统将没有一个完整、安全的数据操作基础，在P2P节点很容易遭到攻击或者发生存储、处理故障的情况下，需要及时的检测当前存储源数据的P2P节点中数据的完整性。通过给P2P节点中的数据加盐度值的方式，验证当前节点所存储的数据是否与源数据相同，是否完整的保存有原始的全部数据。在本方案中源数据用于表

示最初始的数据，即数据存储的标准数据，这些数据存储在本地的服务器中，用于通过这些数据与存储在P2P节点中的数据进行对比，检验P2P节点中数据的正确性。

[0055] 本实施例中将原始数据进行分块之后得到至少两个数据分块，将数据分块发送至网络中对应的存储节点进行存储。其中，发送数据分块的方式可以通过有线传输或者无线传输的方式，其发送的时间可以是在数据分块生成完毕之后发送，也可以是在生成数据分块的同时进行发送，在分块数据的生成过程结束之后，发送分块数据的过程也跟随着结束。

[0056] 我们可以获取原始数据的数据信息，例如数据大小、数据类型等，根据数据大小和数据类型确定数据分块的大小，并且，每个数据分块的大小可以是不一样的，可以根据原始数据的大小和数据类型确定，此处不做限定。同时，我们还可以确定网络中每个存储节点的运行情况，例如内存占用率、存储空间占用率、网络带宽占用率等信息，通过这些信息来衡量一个存储节点的存储情况，并根据每个存储节点的存储情况对该存储节点布置对等的存储任务，保证每个存储节点的正常运行，以及数据存储的高效性和可靠性。

[0057] S2011：确定至少一个数据验证终端；所述数据验证终端用于代替数据所有者终端对存储节点中的存储数据进行验证。

[0058] 在对数据进行验证时，可以是由数据所有者终端亲自进行数据验证，也可以是数据所有者终端来确定至少一个数据验证终端，通过该数据验证终端，来代替数据所有者终端对存储节点中的存储数据进行验证。

[0059] 具体的，数据验证终端可以是网络中的其他存储节点，也可以是管理存储节点的、权限较高的节点，这一类的节点具有较高的权限，可以像数据所有者终端一样获取存储节点中的存储数据、向存储节点发送数据处理指令等。在确定数据验证终端时，数据所有者终端可以是先确定一个数据验证终端的名单，通过在该名单中选择至少一个数据验证终端，来验证存储数据的正确性。

[0060] S2012：发送待验证的存储数据的数据标识至所述数据验证终端，并委托所述数据验证终端对所述数据标识对应的存储数据进行验证。

[0061] 在确定了至少一个数据验证终端来验证存储数据的正确性时，可以发送待验证

的存储数据的数据标识至该数据验证终端，以通知该数据验证终端来验证该数据标识所对应的存储数据，达到委托数据验证终端来验证数据的目的。

[0062] 为了保证第三方数据验证终端验证数据的公平性，数据所有者终端可以确定至少两个数据验证终端来进行数据验证，并同时向确定出来的至少两个数据验证终端发送待验证的存储数据的数据标识，在所有数据验证终端对数据验证结束之后，接收所有数据验证终端发送的验证结果，通过比对多个数据验证结果，来保证第三方数据验证的公平性和客观性。

[0063] S202：对每个所述数据分块进行哈希运算，得到根默克尔哈希。

[0064] 我们通过对数据分块进行哈希运算，得到根默克尔哈希。哈希是一个把任意长度的数据映射成固定长度数据的函数。例如，对于数据完整性校验，最简单的方法是对整个数据做哈希运算得到固定长度的哈希值，然后把得到的哈希值公布在网上，这样用户下载到数据之后，对数据再次进行哈希运算，比较运算结果和网上公布的哈希值进行比较，如果两个计算哈希值相等，说明下载的数据没有损坏。可以这样做是因为输入数据的稍微改变就会引起哈希运算结果的面目全非，而且根据哈希值反推原始输入数据的特征是困难的。

[0065] 由于哈希运算的应用的多样性，它们经常是专为某一应用而设计的。例如，加密散列函数假设存在一个要找到具有相同散列值的原始输入的敌人。一个设计优秀的加密散列函数是一个“单向”操作：对于给定的散列值，没有实用的方法可以计算出一个原始输入，也就是说很难伪造。为加密散列为目的设计的函数，如消息摘要算法（Message-Digest Algorithm，MD5），被广泛的用作检验散列函数。这样软件下载的时候，就会对照验证代码之后才下载正确的文件部分。此代码有可能因为环境因素的变化，如机器配置或者IP地址的改变而有变动，以保证源文件的安全性。

[0066] S203：根据每个所述数据分块及其根默克尔哈希构建默克尔树，并存储所述默克尔树。

[0067] 在得到根默克尔哈希之后，我们根据每个数据分块及其根默克尔哈希构建默克尔树。其中，默克尔树中所有叶子节点都是认证数据的哈希值，每个非叶子节点的散列标签或标签值是根据它下面所有子节点进行组合，然后对组合进行哈

希计算得出。默克尔树是哈希列表和哈希链的泛化。通常在证明一个叶节点是给定默克尔树的一部分时，需要处理的数据量与节点的数量的对数成正比。然而使用哈希表后，需要处理的数据量正比于节点的数量。通过比对本地存储的根节点哈希值来判断数据在位置上是否完整，数据块标签则用来确保数据块在数值上是正确的。为了支持动态数据操作，在计算标签时不应包含文件的索引信息，任何针对单个数据块的操作不会影响到其他的数据块。执行更新操作时，它会检查默克尔树确保更新后的数据块在其正确的位置。

[0068] 由于默克尔哈希的特性，数据存储节点通过缓存少量的中间哈希，即可极大的减少数据证明所需的计算开销。以一个数据分块大小（D）为8M字节，分块大小（B）为64字节的数据例，计算一次数据证明需要执行：(D/B)*2-1-Log(D/B)=262126次哈希计算；若存储节点在第一数据证明计算后，缓存了默克尔树的第3层的8个哈希值，即从数据分块至根默克尔哈希的计算路径，则之后的数据证明只需要执行：(D/8/B)*2-1-Log (D/8/B)+4=32757次哈希计算，约为原来的1/8，因此，本实施例的验证方式可以减少数据计算量并提高数据验证效率。

[0069] 为了保持数据一致，分布系统间数据需要同步，如果对机器上所有数据都进行比对的话，数据传输量就会很大，从而造成“网络拥挤”。为了解决这个问题，可以在每台机器上构造一棵默克尔树，这样，在两台机器间进行数据比对时，从默克尔树的根节点开始进行比对，如果根节点一样，则表示两个副本目前是一致的，不再需要任何处理；如果不一样，则沿着哈希值不同的节点路径查询，很快就能定位到数据不一致的叶节点，只用把不一致的数据同步即可，这样大大节省了比对时间以及数据的传输量。

[0070] 步骤S203可以具体包括S2031~S2034：

[0071] S2031：接收所述存储节点发送的存储数据变化请求；所述存储数据变化请求中包括待改动的存储数据和改动之后的存储数据。

[0072] 在将数据分块计算得到的根默克尔哈希构建默克尔树之后，在实际应用中仍然会出现数据分块发生变化的情况，这种情况会连带造成默克尔树中的根默克尔哈希也会发狠该变化，因此，在数据发生变化的时候，存储节点发送存储数据变化请求至数据所有者终端，其中，存储数据变化请求中包括待改动的存储数

据和改动之后的存储数据，以使数据所有者终端可以确定发生变化的存储数据，并能相应的修改默克尔树。

[0073] S2032：根据所述存储数据变化请求，对所述待改动的存储数据和改动之后的存储数据进行验证。

[0074] 在数据所有者终端接收到存储数据变化请求之后，此为存储节点对数据所有者的数据进行的改动，因此需要经过数据所有者终端的确认和通过。数据所有者终端在接收到数据变化请求之后，根据数据变化请求先确定待改动的存储数据，以及改动之后的存储数据。在确定了之后，对待改动的存储数据和改动之后的存储数据进行验证。

[0075] 具体的，在验证改动数据的过程中，可以先获取发送存储数据变化请求的存储节点的权限，权限可以包括该存储节点可以处理的数据类型、数据标识以及对应的处理方式，根据存储节点的权限、待改动的存储数据和改动之后的存储数据，将其进行对比，确定待改动的存储数据和改动之后的存储数据是否符合该存储节点的权限。

[0076] S2033：若验证通过，则根据所述改动之后的存储数据重新计算根默克尔哈希。

[0077] 若待改动的存储数据和改动之后的存储数据符合该存储节点的权限，则说明验证通过，根据改动之后的存储数据重新计算根默克尔哈希，以根据重新计算出来的根默克尔哈希对默克尔树进行对应的修改。

[0078] 若验证没有通过，则表示改动之后的存储数据不符合该存储节点的数据处理权限，或者被改动的存储数据不是该存储节点的处理权限对象中的数据，对于这种情况，我们可以不对默克尔树进行修改，并向该存储节点发送修改违规通知，以告知该存储节点的数据改动行为违规。

[0079] S2034：根据所述改动之后的存储数据以及重新计算得到根默克尔哈希更新所述默克尔树。

[0080] 在重新计算得到根默克尔哈希之后，根据改动之后的存储数据的数据标识确定该数据标识对应的根默克尔哈希在默克尔树中的位置，再将改动之后的存储数据和重新计算得到的根默克尔哈希对默克尔树进行修改。

[0081] S204：发送数据验证通知至存储待检验的数据分块的存储节点；所述数据验证通知包括所述待检验的数据分块的数据标识。

[0082] 在本实施例中S204与图1对应的实施例中S101的实现方式完全相同，具体可参考图1对应的实施例中的S101的相关描述，在此不再赘述。

[0083] S205：接收所述存储节点根据所述数据标识发送的证明数据；所述证明数据包括所述存储节点中与所述数据标识对应的存储数据，以及根据所述存储数据计算根默克尔哈希的计算路径。

[0084] 在本实施例中S205与图1对应的实施例中S102的实现方式完全相同，具体可参考图1对应的实施例中的S102的相关描述，在此不再赘述。

[0085] S206：根据所述存储数据和所述计算路径，计算根默克尔哈希，并将计算结果与预设的默克尔树中的根默克尔哈希进行比较。

[0086] 在数据所有者对存储节点所持有的数据持有性进行检查时，数据所有者选择一个随机数P，P>= 0且P< D/B；要求存储节点提供数据分块P的原始数据和从数据分块P至根默克尔哈希的计算路径。假设P的数据标识为001，则存储节点需要提供数据分块为Datablock

001的原始数据，以及默克尔哈希计算路径：hash0-0，hash1。数据所有者根据存储节点提供的证明数据，计算根默克尔哈希，并与之前根据原始数据计算的根默克尔哈希进行比较，以确定存储节点是真正保存了该数据。

[0087] 在根据数据分块的地址和数据分块确定目标节点中的数据是否完整的过程中，可以快速比较大量数据，当两个默克尔树根相同时，则意味着所代表的数据必然相同。也可以通过快速定位修改，例如上例中，如果某个数据分块中数据被修改，会影响到hash0-0，hash0和默克尔树根。因此，沿着默克尔树根到hash0，hash0到hash0-0的路径，可以快速定位到发生改变的数据分块。默克尔树可以单独拿出一个分支来，作为一个小树，对部分数据进行校验，这个很多使用场合就带来了哈希列表所不能比拟的方便和高效。正是源于这些优点，默克尔树常用于分布式系统或分布式存储中。

[0088] S207：若根据所述存储数据和所述计算路径计算得到的根默克尔哈希，与所述默克尔树中的根默克尔哈希一致，则判定所述存储节点中的所述存储数据为所

述分块数据。

[0089] 在计算根默克尔哈希之后，将计算结果与预设的默克尔树中的根默克尔哈希进行比较。若根据存储数据和计算路径计算得到的根默克尔哈希，与默克尔树中的根默克尔哈希一致，则判定存储节点中的存储数据为分块数据。

[0090] 步骤S207还可包括步骤S2071~S2072：

[0091] S2071：若根据所述存储数据和所述计算路径计算得到的根默克尔哈希，与预设的默克尔树中的根默克尔哈希不同，则判定所述存储节点中的所述存储数据与所述分块数据不一致，并生成验证失败记录。

[0092] 在计算根默克尔哈希之后，将计算结果与预设的默克尔树中的根默克尔哈希进行比较。若根据存储数据和计算路径计算得到的根默克尔哈希，与预设的默克尔树中的根默克尔哈希不同，则判定存储节点中的存储数据与分块数据不一致，并生成验证失败记录。其中，验证失败记录可以包括存储数据标识、验证失败原因等，此处不做限定。

[0093] S2072：发送所述验证失败记录和所述存储数据对应的分块数据至所述存储节点，并用所述分块数据替换所述存储节点中验证失败的存储数据。

[0094] 当验证失败之后，我们可以判定当前存储节点所存储的存储数据可能与数据所有者终端的原始数据存储出入，这种情况下，我们先确定该存储数据对应的分块数据，再将分块数据发送至存储节点，以通过正确的分块数据替换存储节点中验证失败的存储数据，保证存储节点中的存储数据的正确性和完整性。

[0095] 上述方案，通过对数据所有者终端的原始数据进行分块，并将数据分块存储至对应的存储节点中，在确定了待验证的存储数据之后，根据存储节点发送的存储数据和计算根默克尔哈希的计算路径，计算根默克尔哈希，将计算结果与预先存储的根默克尔哈希进行对比，以确定存储节点所存储的存储数据的正确性，保证了点对点存储过程中存储节点保存数据的持有性和完整性。

[0096] 参见图3，图3是本申请实施例三提供的一种终端设备的示意图。终端设备包括的各单元用于执行图1~图2对应的实施例中的各步骤。具体请参阅图1~图2各自对应的实施例中的相关描述。为了便于说明，仅示出了与本实施例相关的部分。本实施例的终端设备300包括：

[0097] 发送单元301，用于发送数据验证通知至存储待检验的数据分块的存储节点；所述数据验证通知包括所述待检验的数据分块的数据标识；

[0098] 接收单元302，用于接收所述存储节点根据所述数据标识发送的证明数据；所述证明数据包括所述存储节点中与所述数据标识对应的存储数据，以及根据所述存储数据计算根默克尔哈希的计算路径；

[0099] 计算单元303，用于根据所述存储数据和所述计算路径，计算根默克尔哈希，并将计算结果与预设的默克尔树中的根默克尔哈希进行比较；

[0100] 判定单元304，用于若根据所述存储数据和所述计算路径计算得到的根默克尔哈希，与所述默克尔树中的根默克尔哈希一致，则判定所述存储节点中的所述存储数据为所述分块数据。

[0101] 在本实施例中，所述终端设备还可以包括：

[0102] 分块单元，用于对数据所有者终端的原始数据进行分块，得到至少两个数据分块，并将每个所述数据分块发送至网络中对应的存储节点进行存储；

[0103] 哈希计算单元，用于对每个所述数据分块进行哈希运算，得到根默克尔哈希；

[0104] 建树单元，用于根据每个所述数据分块及其根默克尔哈希构建默克尔树，并存储所述默克尔树。

[0105] 在本实施例中，所述终端设备还可以包括：

[0106] 验证单元，用于若根据所述存储数据和所述计算路径计算得到的根默克尔哈希，与预设的默克尔树中的根默克尔哈希不同，则判定所述存储节点中的所述存储数据与所述分块数据不一致，并生成验证失败记录；

[0107] 记录发送单元，用于发送所述验证失败记录和所述存储数据对应的分块数据至所述存储节点，并用所述分块数据替换所述存储节点中验证失败的存储数据。

[0108] 在本实施例中，所述建树单元可以包括：

[0109] 请求接收单元，用于接收所述存储节点发送的存储数据变化请求；所述存储数据变化请求中包括待改动的存储数据和改动之后的存储数据；

[0110] 数据验证单元，用于根据所述存储数据变化请求，对所述待改动的存储数据和改动之后的存储数据进行验证；

[0111] 验证通过单元，用于若验证通过，则根据所述改动之后的存储数据重新计算根

默克尔哈希；

[0112] 数据修改单元，用于根据所述改动之后的存储数据以及重新计算得到根默克尔哈希更新所述默克尔树。

[0113] 在本实施例中，所述终端设备还可以包括：

[0114] 终端确定单元，用于确定至少一个数据验证终端；所述数据验证终端用于代替数据所有者终端对存储节点中的存储数据进行验证；

[0115] 验证委托单元，用于发送待验证的存储数据的数据标识至所述数据验证终端，并委托所述数据验证终端对所述数据标识对应的存储数据进行验证。

[0116] 上述方案，通过发送数据验证通知至存储待检验的数据分块的存储节点，接收存储节点根据数据标识发送的证明数据；证明数据包括存储节点中与数据标识对应的存储数据，以及根据存储数据计算根默克尔哈希的计算路径；根据存储数据和计算路径计算根默克尔哈希，并将计算结果与预设的默克尔树中的根默克尔哈希进行比较；若根据存储数据和计算路径计算得到的根默克尔哈希，与默克尔树中的根默克尔哈希一致，则判定存储节点中的存储数据为分块数据。根据数据分块对应的存储数据以及数据分块在预存的默克尔树中的计算路径，判断数据分块在目标节点中是否存储正确，保证了点对点存储过程中存储节点保存数据的持有性和正确性。

[0117] 参照图4，示出了本申请一个实施例的一种终端设备的示意图。如图4所示，本实施例的终端设备400包括：处理器410、存储器420以及存储在所述存储器420中并可在所述处理器410上运行的计算机可读指令421。所述处理器410执行所述计算机可读指令421时实现上述数据持有性验证方法各个实施例中的步骤，例如图1所示的步骤S101至S104。或者，所述处理器410执行所述计算机可读指令421时实现上述各装置实施例中各模块/单元的功能，例如图3所示单元301至304的功能。

[0118] 示例性的，所述计算机可读指令421可以被分割成一个或多个模块/单元，所述一个或者多个模块/单元被存储在所述存储器420中，并由所述处理器410执行，以完成本申请。所述一个或多个模块/单元可以是能够完成特定功能的一系列计算机可读指令段，该指令段可以用于描述所述计算机可读指令421在所述终端设

备400中的执行过程。例如，所述计算机可读指令421可以被分割成发送单元、接收单元、计算单元、判定单元，各单元具体功能如下：

[0119] 发送单元，用于发送数据验证通知至存储待检验的数据分块的存储节点；所述数据验证通知包括所述待检验的数据分块的数据标识；

[0120] 接收单元，用于接收所述存储节点根据所述数据标识发送的证明数据；所述证明数据包括所述存储节点中与所述数据标识对应的存储数据，以及根据所述存储数据计算根默克尔哈希的计算路径；

[0121] 计算单元，用于根据所述存储数据和所述计算路径，计算根默克尔哈希，并将计算结果与预设的默克尔树中的根默克尔哈希进行比较；

[0122] 判定单元，用于若根据所述存储数据和所述计算路径计算得到的根默克尔哈希，与所述默克尔树中的根默克尔哈希一致，则判定所述存储节点中的所述存储数据为所述分块数据。

[0123] 所述终端设备400可以是桌上型计算机、笔记本、掌上电脑及云端服务器等计算设备。所述终端设备400可包括，但不仅限于，处理器410、存储器420。本领域技术人员可以理解，图4仅仅是终端设备400的一种示例，并不构成对终端设备400的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件，例如所述终端设备400还可以包括输入输出设备、网络接入设备、总线等。

[0124] 所述处理器410可以是中央处理单元（Central Processing Unit，CPU），还可以是其他通用处理器、数字信号处理器（Digital Signal Processor，DSP）、专用集成电路（Application Specific Integrated Circuit，ASIC）、现成可编程门阵列（Field-Programmable Gate Array，FPGA）或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。

[0125] 所述存储器420可以是所述终端设备400的内部存储单元，例如终端设备400的硬盘或内存。所述存储器420也可以是所述终端设备400的外部存储设备，例如所述终端设备400上配备的插接式硬盘，智能存储卡（Smart Media Card, SMC），安全数字（Secure Digital, SD）卡，闪存卡（Flash Card）等等。进一步地，所

述存储器420还可以既包括所述终端设备400的内部存储单元也包括外部存储设备。所述存储器420用于存储所述计算机可读指令421以及所述终端设备400所需的其他指令和数据。所述存储器420还可以用于暂时地存储已经输出或者将要输出的数据。

[0126] 本领域普通技术人员可以理解，实现上述实施例方法中的全部或部分流程，是可以通过计算机可读指令来指令相关的硬件来完成，所述的计算机可读指令可存储于一非易失性计算机可读取存储介质中，该计算机可读指令在执行时，可包括如上述各方法的实施例的流程。其中，本申请所提供的各实施例中所使用的对存储器、存储、数据库或其它介质的任何引用，均可包括非易失性和/或易失性存储器。非易失性存储器可包括只读存储器（ROM）、可编程ROM（PROM）、电可编程ROM（EPROM）、电可擦除可编程ROM（EEPROM）或闪存。易失性存储器可包括随机存取存储器（RAM）或者外部高速缓冲存储器。作为说明而非局限，RAM以多种形式可得，诸如静态RAM（SRAM）、动态RAM（DRAM）、同步DRAM（SDRAM）、双数据率SDRAM（DDRSDRAM）、增强型SDRAM（ESDRAM）、同步链路（Synchlink）DRAM（SLDRAM）、存储器总线（Rambus）直接RAM（RDRAM）、直接存储器总线动态RAM（DRDRAM）、以及存储器总线动态RAM（RDRAM）等。

[0127] 以上所述实施例仅用以说明本申请的技术方案，而非对其限制；尽管参照前述实施例对本申请进行了详细的说明，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申请各实施例技术方案的精神和范围，均应包含在本申请的保护范围之内。

权利要求书

[权利要求 1] 一种数据持有性验证方法，其特征在于，包括：

发送数据验证通知至存储待检验的数据分块的存储节点；所述数据验证通知包括所述待检验的数据分块的数据标识；

接收所述存储节点根据所述数据标识发送的证明数据；所述证明数据包括所述存储节点中与所述数据标识对应的存储数据，以及根据所述存储数据计算根默克尔哈希的计算路径；

根据所述存储数据和所述计算路径，计算根默克尔哈希，并将计算结果与预设的默克尔树中的根默克尔哈希进行比较；

若根据所述存储数据和所述计算路径计算得到的根默克尔哈希，与所述预设的默克尔树中的根默克尔哈希一致，则判定所述存储节点中的所述存储数据为所述分块数据。

[权利要求 2] 如权利要求1所述的数据持有性验证方法，其特征在于，所述发送数据验证通知至存储待检验的数据分块的存储节点之前，还包括：

对数据所有者终端的原始数据进行分块，得到至少两个数据分块，并将每个所述数据分块发送至网络中对应的存储节点进行存储；

对每个所述数据分块进行哈希运算，得到根默克尔哈希；

根据每个所述数据分块及其根默克尔哈希构建默克尔树，并存储所述默克尔树。

[权利要求 3] 如权利要求1所述的数据持有性验证方法，其特征在于，所述根据所述存储数据和所述计算路径，计算根默克尔哈希，并将计算结果与预设的默克尔树中的根默克尔哈希进行比较之后，还包括：

若根据所述存储数据和所述计算路径计算得到的根默克尔哈希，与预设的默克尔树中的根默克尔哈希不同，则判定所述存储节点中的所述存储数据与所述分块数据不一致，并生成验证失败记录；

发送所述验证失败记录和所述存储数据对应的分块数据至所述存储节点，并用所述分块数据替换所述存储节点中验证失败的存储数据。

[权利要求 4] 如权利要求2所述的数据持有性验证方法，其特征在于，所述根据每

个所述数据分块及其根默克尔哈希构建默克尔树，并存储所述默克尔树，包括：

接收所述存储节点发送的存储数据变化请求；所述存储数据变化请求中包括待改动的存储数据和改动之后的存储数据；

根据所述存储数据变化请求，对所述待改动的存储数据和改动之后的存储数据进行验证；

若验证通过，则根据所述改动之后的存储数据重新计算根默克尔哈希；

根据所述改动之后的存储数据以及重新计算得到根默克尔哈希更新所述默克尔树。

[权利要求 5] 如权利要求1-4任一项所述的数据持有性验证方法，其特征在于，所述发送数据验证通知至存储待检验的数据分块的存储节点之前，还包括：

确定至少一个数据验证终端；所述数据验证终端用于代替数据所有者终端对存储节点中的存储数据进行验证；

发送待验证的存储数据的数据标识至所述数据验证终端，并委托所述数据验证终端对所述数据标识对应的存储数据进行验证。

[权利要求 6] 一种终端设备，其特征在于，包括存储器以及处理器，所述存储器中存储有可在所述处理器上运行的计算机可读指令，其特征在于，所述处理器执行所述计算机可读指令时实现如下步骤：

发送数据验证通知至存储待检验的数据分块的存储节点；所述数据验证通知包括所述待检验的数据分块的数据标识；

接收所述存储节点根据所述数据标识发送的证明数据；所述证明数据包括所述存储节点中与所述数据标识对应的存储数据，以及根据所述存储数据计算根默克尔哈希的计算路径；

根据所述存储数据和所述计算路径，计算根默克尔哈希，并将计算结果与预设的默克尔树中的根默克尔哈希进行比较；

若根据所述存储数据和所述计算路径计算得到的根默克尔哈希，与所

述默克尔树中的根默克尔哈希一致，则判定所述存储节点中的所述存储数据为所述分块数据。

[权利要求 7] 根据权利要求6所述的终端设备，其特征在于，所述处理器执行所述计算机可读指令时还实现如下步骤：

对数据所有者终端的原始数据进行分块，得到至少两个数据分块，并将每个所述数据分块发送至网络中对应的存储节点进行存储；

对每个所述数据分块进行哈希运算，得到根默克尔哈希；

根据每个所述数据分块及其根默克尔哈希构建默克尔树，并存储所述默克尔树。

[权利要求 8] 根据权利要求6所述的终端设备，其特征在于，所述处理器执行所述计算机可读指令时还实现如下步骤：

若根据所述存储数据和所述计算路径计算得到的根默克尔哈希，与预设的默克尔树中的根默克尔哈希不同，则判定所述存储节点中的所述存储数据与所述分块数据不一致，并生成验证失败记录；

发送所述验证失败记录和所述存储数据对应的分块数据至所述存储节点，并用所述分块数据替换所述存储节点中验证失败的存储数据。

[权利要求 9] 根据权利要求7所述的终端设备，其特征在于，所述处理器执行所述计算机可读指令时还实现如下步骤：

接收所述存储节点发送的存储数据变化请求；所述存储数据变化请求中包括待改动的存储数据和改动之后的存储数据；

根据所述存储数据变化请求，对所述待改动的存储数据和改动之后的存储数据进行验证；

若验证通过，则根据所述改动之后的存储数据重新计算根默克尔哈希；

根据所述改动之后的存储数据以及重新计算得到根默克尔哈希更新所述默克尔树。

[权利要求 10] 根据权利要求6-9任一项所述的终端设备，其特征在于，所述处理器执行所述计算机可读指令时还实现如下步骤：

确定至少一个数据验证终端；所述数据验证终端用于代替数据所有者终端对存储节点中的存储数据进行验证；

发送待验证的存储数据的数据标识至所述数据验证终端，并委托所述数据验证终端对所述数据标识对应的存储数据进行验证。

[权利要求 11] 一种终端设备，其特征在于，包括：

发送单元，用于发送数据验证通知至存储待检验的数据分块的存储节点；所述数据验证通知包括所述待检验的数据分块的数据标识；

接收单元，用于接收所述存储节点根据所述数据标识发送的证明数据；所述证明数据包括所述存储节点中与所述数据标识对应的存储数据，以及根据所述存储数据计算根默克尔哈希的计算路径；

计算单元，用于根据所述存储数据和所述计算路径，计算根默克尔哈希，并将计算结果与预设的默克尔树中的根默克尔哈希进行比较；

判定单元，用于若根据所述存储数据和所述计算路径计算得到的根默克尔哈希，与所述默克尔树中的根默克尔哈希一致，则判定所述存储节点中的所述存储数据为所述分块数据。

[权利要求 12] 根据权利要求11所述的终端设备，其特征在于，还包括：

分块单元，用于对数据所有者终端的原始数据进行分块，得到至少两个数据分块，并将每个所述数据分块发送至网络中对应的存储节点进行存储；

哈希计算单元，用于对每个所述数据分块进行哈希运算，得到根默克尔哈希；

建树单元，用于根据每个所述数据分块及其根默克尔哈希构建默克尔树，并存储所述默克尔树。

[权利要求 13] 根据权利要求11所述的终端设备，其特征在于，还包括：

验证单元，用于若根据所述存储数据和所述计算路径计算得到的根默克尔哈希，与预设的默克尔树中的根默克尔哈希不同，则判定所述存储节点中的所述存储数据与所述分块数据不一致，并生成验证失败记录；

记录发送单元，用于发送所述验证失败记录和所述存储数据对应的分块数据至所述存储节点，并用所述分块数据替换所述存储节点中验证失败的存储数据。

[权利要求 14] 根据权利要求12所述的终端设备，其特征在于，还包括：

请求接收单元，用于接收所述存储节点发送的存储数据变化请求；所述存储数据变化请求中包括待改动的存储数据和改动之后的存储数据；

数据验证单元，用于根据所述存储数据变化请求，对所述待改动的存储数据和改动之后的存储数据进行验证；

验证通过单元，用于若验证通过，则根据所述改动之后的存储数据重新计算根默克尔哈希；

数据修改单元，用于根据所述改动之后的存储数据以及重新计算得到根默克尔哈希更新所述默克尔树。

[权利要求 15] 根据权利要求11-14任一项所述的终端设备，其特征在于，还包括：

终端确定单元，用于确定至少一个数据验证终端；所述数据验证终端用于代替数据所有者终端对存储节点中的存储数据进行验证；

验证委托单元，用于发送待验证的存储数据的数据标识至所述数据验证终端，并委托所述数据验证终端对所述数据标识对应的存储数据进行验证。

[权利要求 16] 一种计算机非易失性可读存储介质，所述计算机非易失性可读存储介质存储有计算机可读指令，其特征在于，所述计算机可读指令被处理器执行时实现如下步骤：

发送数据验证通知至存储待检验的数据分块的存储节点；所述数据验证通知包括所述待检验的数据分块的数据标识；

接收所述存储节点根据所述数据标识发送的证明数据；所述证明数据包括所述存储节点中与所述数据标识对应的存储数据，以及根据所述存储数据计算根默克尔哈希的计算路径；

根据所述存储数据和所述计算路径，计算根默克尔哈希，并将计算结

果与预设的默克尔树中的根默克尔哈希进行比较；

若根据所述存储数据和所述计算路径计算得到的根默克尔哈希，与所述预设的默克尔树中的根默克尔哈希一致，则判定所述存储节点中的所述存储数据为所述分块数据。

[权利要求 17] 根据权利要求16所述的计算机非易失性可读存储介质，其特征在于，所述计算机可读指令被处理器执行时还实现如下步骤：

对数据所有者终端的原始数据进行分块，得到至少两个数据分块，并将每个所述数据分块发送至网络中对应的存储节点进行存储；

对每个所述数据分块进行哈希运算，得到根默克尔哈希；

根据每个所述数据分块及其根默克尔哈希构建默克尔树，并存储所述默克尔树。

[权利要求 18] 根据权利要求16所述的计算机非易失性可读存储介质，其特征在于，所述计算机可读指令被处理器执行时还实现如下步骤：

若根据所述存储数据和所述计算路径计算得到的根默克尔哈希，与预设的默克尔树中的根默克尔哈希不同，则判定所述存储节点中的所述存储数据与所述分块数据不一致，并生成验证失败记录；

发送所述验证失败记录和所述存储数据对应的分块数据至所述存储节点，并用所述分块数据替换所述存储节点中验证失败的存储数据。

[权利要求 19] 根据权利要求17所述的计算机非易失性可读存储介质，其特征在于，所述计算机可读指令被处理器执行时还实现如下步骤：

接收所述存储节点发送的存储数据变化请求；所述存储数据变化请求中包括待改动的存储数据和改动之后的存储数据；

根据所述存储数据变化请求，对所述待改动的存储数据和改动之后的存储数据进行验证；

若验证通过，则根据所述改动之后的存储数据重新计算根默克尔哈希；

根据所述改动之后的存储数据以及重新计算得到根默克尔哈希更新所述默克尔树。

[权利要求 20] 根据权利要求16-19任一项所述的计算机非易失性可读存储介质，其特征在于，所述计算机可读指令被处理器执行时还实现如下步骤：

确定至少一个数据验证终端；所述数据验证终端用于代替数据所有者终端对存储节点中的存储数据进行验证；

发送待验证的存储数据的数据标识至所述数据验证终端，并委托所述数据验证终端对所述数据标识对应的存储数据进行验证。

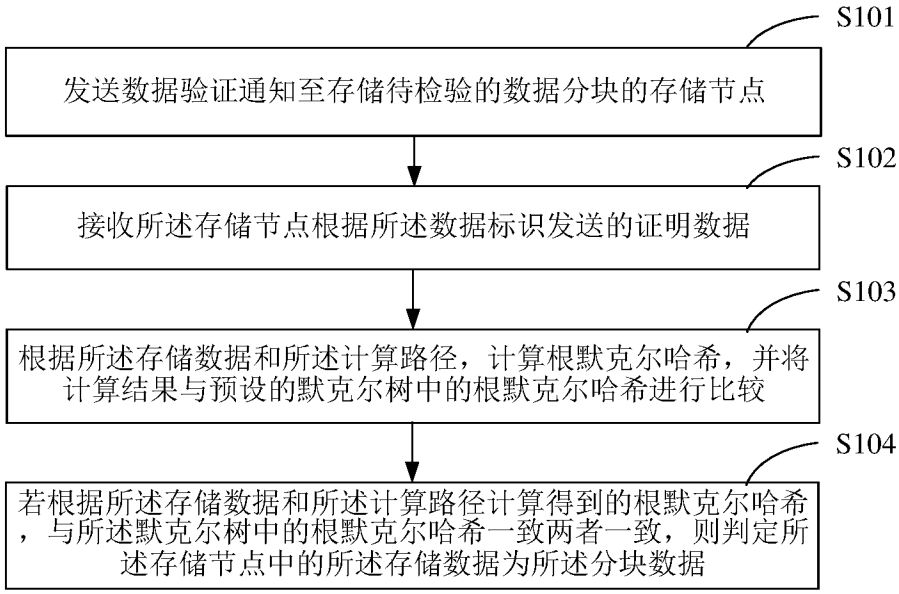
S101
发送数据验证通知至存储待检验的数据分块的存储节点
S102
接收所述存储节点根据所述数据标识发送的证明数据
S103
根据所述存储数据和所述计算路径，计算根默克尔哈希，并将计算结果与预设的默克尔树中的根默克尔哈希进行比较
S104
若根据所述存储数据和所述计算路径计算得到的根默克尔哈希，与所述默克尔树中的根默克尔哈希一致两者一致，则判定所述存储节点中的所述存储数据为所述分块数据

图 1

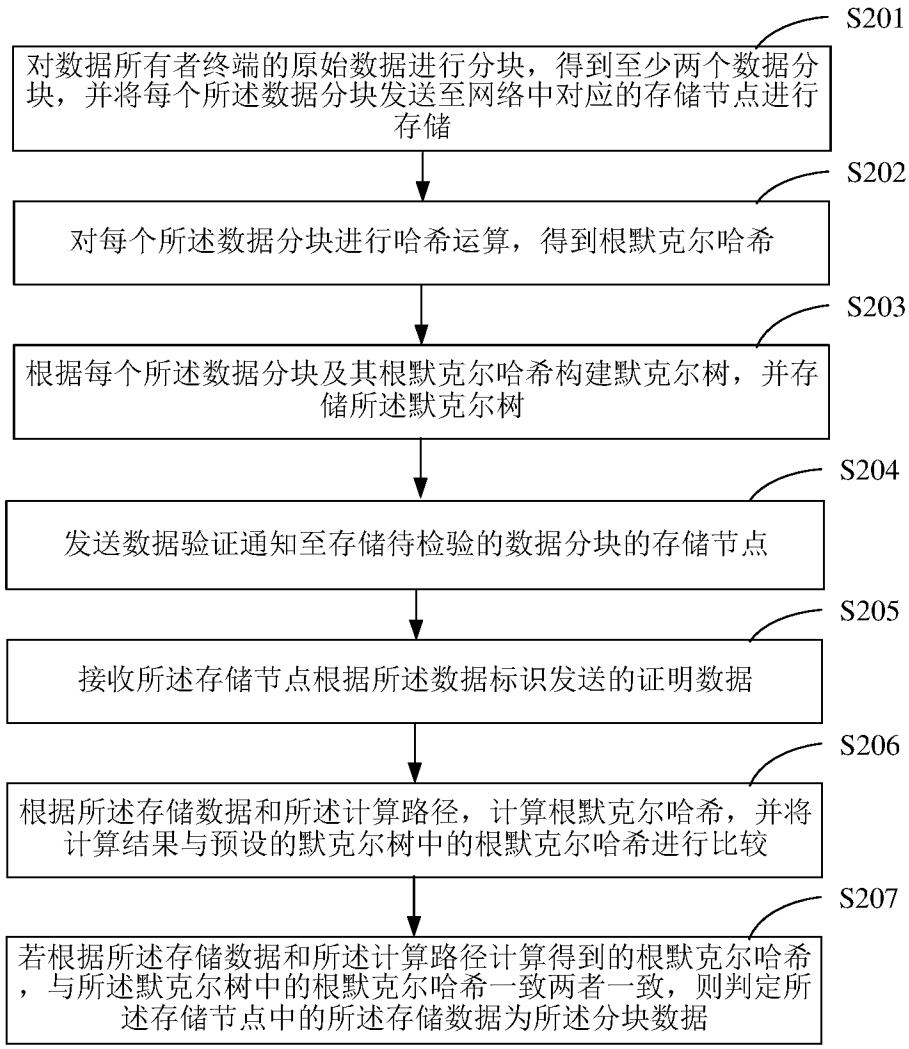
S201
对数据所有者终端的原始数据进行分块，得到至少两个数据分块，并将每个所述数据分块发送至网络中对应的存储节点进行存储
S202
对每个所述数据分块进行哈希运算，得到根默克尔哈希
S203
根据每个所述数据分块及其根默克尔哈希构建默克尔树，并存储所述默克尔树
S204
发送数据验证通知至存储待检验的数据分块的存储节点
S205
接收所述存储节点根据所述数据标识发送的证明数据
S206
根据所述存储数据和所述计算路径，计算根默克尔哈希，并将计算结果与预设的默克尔树中的根默克尔哈希进行比较
S207
若根据所述存储数据和所述计算路径计算得到的根默克尔哈希，与所述默克尔树中的根默克尔哈希一致两者一致，则判定所述存储节点中的所述存储数据为所述分块数据

图 2

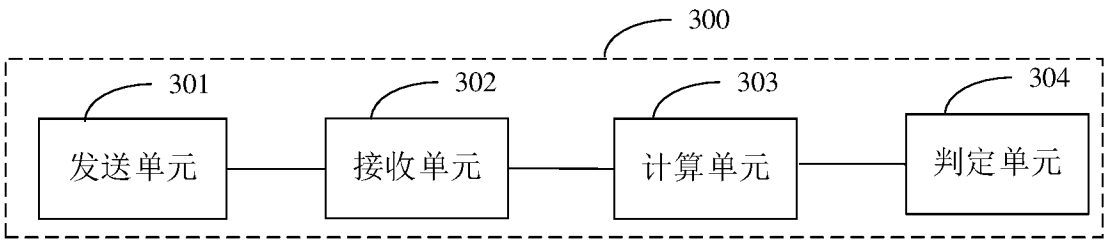
300
301
发送单元
302
接收单元
303
计算单元
304
判定单元

图 3

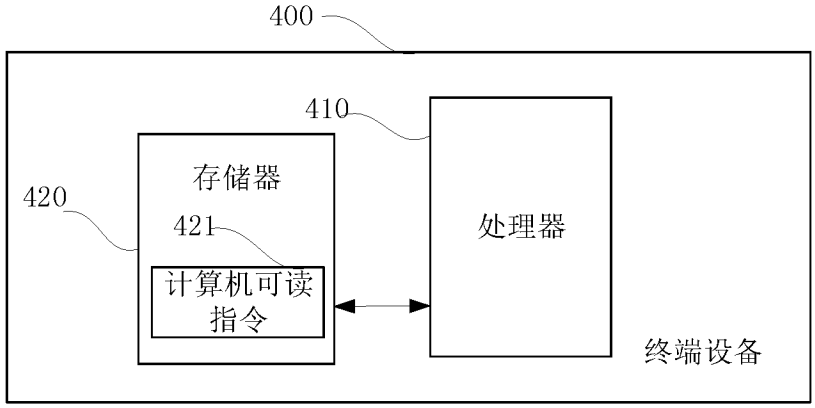

图 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2019/118146

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L;G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, CNKI, WPI, EPODOC: 存在, 持有, 保存, 云, 存储, 证明, 验证, 检验, 查询, 梅克尔, 默克尔, 路径, 分片, 数据, 分块, 哈希, 树, 根, cloud, storage, save, test, data, persistence, Merkle, hash, tree, path, root, PDP, provable data possession

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 109889505 A (PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) 14 June 2019 (2019-06-14) claims 1-10	1-20
X	CN 108664221 A (BEIJING QIHOO TECHNOLOGY CO., LTD.) 16 October 2018 (2018-10-16) description, paragraphs [0043]-[0070]	1-20
A	CN 108681583 A (BEIJING QIHOO TECHNOLOGY CO., LTD.) 19 October 2018 (2018-10-19) entire document	1-20
A	CN 103268460 A (BEIHANG UNIVERSITY) 28 August 2013 (2013-08-28) entire document	1-20
A	CN 106845280 A (GUANGDONG UNIVERSITY OF TECHNOLOGY) 13 June 2017 (2017-06-13) entire document	1-20
A	WO 2010011342 A1 (BROWN UNIVERSITY) 28 January 2010 (2010-01-28) entire document	1-20

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 January 2020	**01 February 2020**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration (ISA/CN) **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2019/118146

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 109889505 A	14 June 2019	None	
CN 108664221 A	16 October 2018	None	
CN 108681583 A	19 October 2018	None	
CN 103268460 A	28 August 2013	CN 103268460 B	10 February 2016
CN 106845280 A	13 June 2017	None	
WO 2010011342 A1	28 January 2010	US 2013198854 A1	01 August 2013
		US 8978155 B2	10 March 2015
		CA 2731954 A1	28 January 2010
		CA 2731954 C	21 October 2014

国际检索报告

国际申请号
PCT/CN2019/118146

A. 主题的分类

H04L 29/06(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L;G06F

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

CNPAT, CNKI, WPI, EPODOC：存在，持有，保存，云，存储，证明，验证，检验，查询，梅克尔，默克尔，路径，分片，数据，分块，哈希，树，根，cloud, storage, save, test, data, persistence, Merkle, hash, tree, path, root, PDP, provable data possession

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
PX	CN 109889505 A (平安科技深圳有限公司) 2019年 6月 14日 (2019-06-14) 权利要求1-10	1-20
X	CN 108664221 A (北京奇虎科技有限公司) 2018年 10月 16日 (2018-10-16) 说明书第0043段-第0070段	1-20
A	CN 108681583 A (北京奇虎科技有限公司) 2018年 10月 19日 (2018-10-19) 全文	1-20
A	CN 103268460 A (北京航空航天大学) 2013年 8月 28日 (2013-08-28) 全文	1-20
A	CN 106845280 A (广东工业大学) 2017年 6月 13日 (2017-06-13) 全文	1-20
A	WO 2010011342 A1 (BROWN UNIVERSITY) 2010年 1月 28日 (2010-01-28) 全文	1-20

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2020年 1月 16日	2020年 2月 1日
ISA/CN的名称和邮寄地址 中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 王侠 电话号码 86-10-53961750

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2019/118146

检索报告引用的专利文件	公布日 (年/月/日)	同族专利	公布日 (年/月/日)
CN 109889505 A	2019年 6月 14日	无	
CN 108664221 A	2018年 10月 16日	无	
CN 108681583 A	2018年 10月 19日	无	
CN 103268460 A	2013年 8月 28日	CN 103268460 B	2016年 2月 10日
CN 106845280 A	2017年 6月 13日	无	
WO 2010011342 A1	2010年 1月 28日	US 2013198854 A1	2013年 8月 1日
		US 8978155 B2	2015年 3月 10日
		CA 2731954 A1	2010年 1月 28日
		CA 2731954 C	2014年 10月 21日