(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 10 月 8 日 (08.10.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/199713 A1

(51) 国际专利分类号:
G06F 21/64 (2013.01)

(21) 国际申请号: PCT/CN2020/071219

(22) 国际申请日: 2020 年 1 月 9 日 (09.01.2020)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910273141.3 2019年4月4日 (04.04.2019) CN

(71) 申请人: 创新先进技术有限公司 (**ADVANCED NEW TECHNOLOGIES CO., LTD.**) [—/CN]; 开曼群岛大开曼岛乔治镇医院路 27 号开曼企业中心, Cayman KY1-9008 (KY)。

(72) 发明人: 杨新颖 (**YANG, Xinying**); 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。

(74) 代理人: 北京博思佳知识产权代理有限公司 (**BEIJING BESTIPR INTELLECTUAL PROPERTY LAW CORPORATION**); 中国北京市海淀区上地三街 9 号嘉华大厦 B 座 409, Beijing 100085 (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, 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,

(54) **Title:** DATA VERIFICATION METHOD, SYSTEM, APPARATUS, AND DEVICE

(54) **发明名称**: 数据验证方法、系统、装置及设备

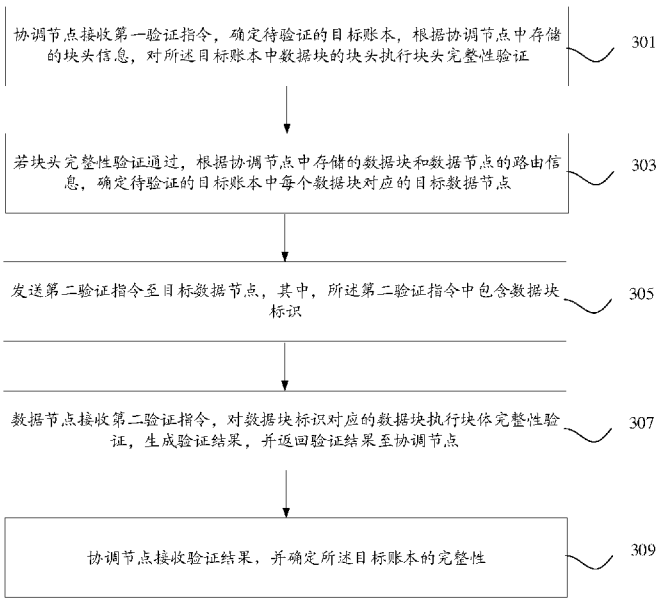


图 3

(57) **Abstract:** A data verification method, a system, an apparatus, and a device. When a blockchain-based account book needs to be verified, integrity verification can first be performed on block headers solely in a coordination node, and after the verification is passed, a further second verification instruction can be issued to each of a plurality of data nodes, so as to cause each data node to execute verification of the interior of the data blocks in parallel.

(57) **摘要**: 一种数据验证方法、系统、装置及设备，当需要对块链式的账本进行验证时，可以首先只在协调节点中对块头进行完整性验证，验证通过之后，再分发进一步的第二验证指令至各数据节点中，让各数据节点并行执行数据块内部的验证。

[见续页]

WO 2020/199713 A1

PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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))。

数据验证方法、系统、装置及设备

技术领域

[01]本说明书实施例涉及信息技术领域，尤其涉及数据验证方法、系统、装置及设备。

背景技术

[02]在对块链式的账本进行完整性验证时，需要按照成块顺序依序对每个数据块进行验证，才能完成一段账本或者全量账本的完整性验证，在待验证的账本中数据块较多以及数据块中数据记录较多的时候，这种验证效率较低。

[03]基于此，需要一种在块链式账本中更为高效的数据验证方式。

发明内容

[04]本申请实施例的目的是提供一种块链式账本中实现高数据验证的方法。

[05]为解决上述技术问题，本申请实施例是这样实现的：

[06]一种数据验证方法，应用于中心化存储块链式账本的数据库系统中，所述数据库系统包括协调节点和数据节点，所述方法包括：

[07]协调节点接收第一验证指令，确定待验证的目标账本，根据协调节点中存储的块头信息，对所述目标账本中数据块的块头执行块头完整性验证，所述目标账本包括部分账本或者全量账本；

[08]若块头完整性验证通过，根据协调节点中存储的数据块和数据节点的路由信息，确定待验证的目标账本中每个数据块对应的目标数据节点，

[09]发送第二验证指令至目标数据节点，其中，所述第二验证指令中包含数据块标识；

[10]数据节点接收第二验证指令，对数据块标识对应的数据块执行块体完整性验证，生成验证结果，并返回验证结果至协调节点；

[11]协调节点接收验证结果，并确定所述目标账本的完整性；

[12]其中，在所述块链式账本中，数据块包含用于存储元数据的块头，和，用于存储数据记录的块体；除初始数据块以外，每一数据块中包含至少一条数据记录，每一数据块中包含由前一数据块的哈希值和自身所包含的数据记录确定的自身数据块的块哈希值，

数据块的块高基于成块时间的先后顺序单调递增。

[13]一种数据验证系统，应用于中心化存储块链式账本的数据库系统中，所述数据库系统包括协调节点和数据节点，

[14]协调节点接收第一验证指令，确定待验证的目标账本，根据协调节点中存储的块头信息，对所述目标账本中数据块的块头执行块头完整性验证，所述目标账本包括部分账本或者全量账本；

[15]若块头完整性验证通过，根据协调节点中存储的数据块和数据节点的路由信息，确定待验证的目标账本中每个数据块对应的目标数据节点，

[16]发送第二验证指令至目标数据节点，其中，所述第二验证指令中包含数据块标识；

[17]数据节点接收第二验证指令，对数据块标识对应的数据块执行块体完整性验证，生成验证结果，并返回验证结果至协调节点；

[18]协调节点接收验证结果，并确定所述目标账本的完整性；

[19]其中，在所述块链式账本中，数据块包含用于存储元数据的块头，和，用于存储数据记录的块体；除初始数据块以外，每一数据块中包含至少一条数据记录，每一数据块中包含由前一数据块的哈希值和自身所包含的数据记录确定的自身数据块的块哈希值，数据块的块高基于成块时间的先后顺序单调递增。

[20]一种数据验证方法，应用于中心化存储块链式账本的数据库系统中的协调节点中，所述方法包括：

[21]接收第一验证指令，确定待验证的目标账本，根据协调节点中存储的块头信息，对所述目标账本中数据块的块头执行块头完整性验证，所述目标账本包括部分账本或者全量账本；

[22]若块头完整性验证通过，根据协调节点中存储的数据块和数据节点的路由信息，确定待验证的目标账本中每个数据块对应的目标数据节点，

[23]发送第二验证指令至目标数据节点，其中，所述第二验证指令中包含数据块标识。

[24]一种数据验证装置，应用于中心化存储块链式账本的数据库系统中的协调节点中，所述装置包括：

[25]块头验证模块，接收第一验证指令，确定待验证的目标账本，根据协调节点中存储的块头信息，对所述目标账本中数据块的块头执行块头完整性验证，所述目标账本包括

部分账本或者全量账本;

[26]确定模块，若块头完整性验证通过，根据协调节点中存储的数据块和数据节点的路由信息，确定待验证的目标账本中每个数据块对应的目标数据节点，

[27]发送模块，发送第二验证指令至目标数据节点，其中，所述第二验证指令中包含数据块标识。

[28]通过本说明书实施例所提供的方案，当需要到对块链式的账本进行验证时，可以首先只在协调节点中对块头进行完整性验证，验证通过之后，再分发进一步的第二验证指令至各数据节点中，让各数据节点并行执行数据块内部的验证，从而可以大幅提高验证效率。

[29]应当理解的是，以上的一般描述和后文的细节描述仅是示例性和解释性的，并不能限制本说明书实施例。

[30]此外，本说明书实施例中的任一实施例并不需要达到上述的全部效果。

附图说明

[31]为了更清楚地说明本说明书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简单地介绍，显而易见地，下面描述中的附图仅仅是本说明书实施例中记载的一些实施例，对于本领域普通技术人员来讲，还可以根据这些附图获得其他的附图。

[32]图 1 为本说明书实施例中所涉及的系统架构的示意图;

[33]图 2 为本说明书实施例所提供的一种关于块头的示意图;

[34]图 3 为本说明书实施例所提供的应用于数据库系统中的数据验证方法的流程示意图;

[35]图 4 为本说明书实施例所提供的应用于协调节点中的数据验证方法的流程示意图;

[36]图 5 为本说明书实施例所提供的应用于协调节点中的数据验证装置的结构示意图;

[37]图 6 是用于配置本说明书实施例方法的一种设备的结构示意图。

具体实施方式

[38]为了使本领域技术人员更好地理解本说明书实施例中的技术方案，下面将结合本说明书实施例中的附图，对本说明书实施例中的技术方案进行详细地描述，显然，所描述

的实施例仅仅是本说明书的一部分实施例，而不是全部的实施例。基于本说明书中的实施例，本领域普通技术人员所获得的所有其他实施例，都应当属于保护的范围。

[39]以下结合附图，详细说明本说明书各实施例提供的技术方案。

[40]首先需要说明的是，本说明书中的数据库系统是以中心化的形式提供数据服务。在当前的服务器架构中，数据库服务器可以是直接对接的客户端个人用户，也可以是由一些应用服务器对接客户端个人用户，而数据库服务器则对接所述应用服务器。在本说明书实施例所涉及的数据库系统中，一个协调节点可以对应于多个数据节点，如图1所示，图1为本说明书实施例中所涉及的系统架构的示意图。

[41]在本说明书实施例所涉及中心化的数据库系统中，数据块可以通过如下方式预先生成：

[42]接收待存储的数据记录，确定各数据记录的哈希值。此处的待存储的数据记录，可以是客户端个人用户的各种消费记录，也可以是应用服务器基于用户的指令，在执行业务逻辑时产生的业务结果、中间状态以及操作记录等等。具体的业务场景可以包括消费记录、审计日志、供应链条、政府监管记录、医疗记录等等。

[43]当达到预设的成块条件时，确定待写入数据块中的各数据记录，生成包含数据块的哈希值和数据记录的第N个数据块。

[44]所述预设的成块条件包括：待存储的数据记录数量达到数量阈值，例如，每接收到一千条数据记录时，生成一个新数据块，将一千条数据记录写入块中；或者，距离上一次成块时刻的时间间隔达到时间阈值，例如，每隔5分钟，生成一个新数据块，将在这5分钟内接收到的数据记录写入块中。

[45]此处的N指的是数据块的序号，换言之，在本说明书实施例中，数据块是以块链的形式，基于成块时间的顺序先后排列，具有很强的时序特征。其中，数据块的块高基于成块时间的先后顺序单调递增。块高可以是序号，此时第N个数据块的块高即为N；块高也可以其它方式生成。

[46]当N=1时，即此时的数据块为为初始数据块。初始数据块的哈希值和块高基于预设方式给定。例如，初始数据块中不包含数据记录，哈希值则为任一给定的哈希值，块高blknum=0；又例如，初始数据块的生成触发条件与其它数据块的触发条件一致，但是初始数据块的哈希值由对初始数据块中的所有内容取哈希确定。

[47]当N>1时，由于前一数据块的内容和哈希值已经确定，则此时，可以基于前一数据

块（即第 N－1 个数据块）的哈希值生成当前数据块（第 N 个数据块）的哈希值，例如，一种可行的方式为，确定每一条将要写入第 N 个块中的数据记录的哈希值，按照在块中的排列顺序，生成一个默克尔树，将默克尔树的根哈希值和前一数据块的哈希值拼接在一起，再次采用哈希算法，生成当前块的哈希值，以及，还可以根据默克尔树的根哈希值和其它一些元数据（例如版本号、数据块的生成时间戳、父数据块哈希等等）生成当前块的哈希值。

[48]又例如，还可以按照块中数据记录的顺序进行拼接并取哈希得到整体数据记录的哈希值，拼接前一数据块的哈希值和整体数据记录的哈希值，并对拼接得到的字串进行哈希运算，生成数据块的哈希值。

[49]在每一个数据块中，其包含用于存储元数据的块头，和，用于存储数据记录的块体。数据块中的块头可以用于存储诸如父哈希、自身的块哈希值、版本号、数据记录的根哈希、时间戳等等。如图 2 所示，图 2 为本说明书实施例所提供的一种关于块头的示意图，当然，块头的格式是可以基于业务需要进行自定义的，其还可以包含一些其它的信息，例如，用于描述数据记录状态的状态数组等等。而块体中则用于存储数据记录的明文或者数据记录的哈希值。

[50]通过前述的数据块的生成方式，每一个数据块通过哈希值确定，数据块的哈希值由数据块中的数据记录的内容、顺序以及前一数据块的哈希值决定。用户可以随时基于数据块的哈希值发起验证，对于数据块中任何内容（包括对于数据块中数据记录内容或者顺序的修改）的修改都会造成在验证时计算得到的数据块的哈希值和数据块生成时的哈希值不一致，而导致验证失败，从而实现了中心化下的不可篡改。

[51]需要说明的是，上述数据块的生成可以是在协调节点中实现，也可以不是在协调节点中实现。例如，数据系统中还可以包含其他业务节点，专门用于处理数据块的生成，以实现业务解耦，每生成一个数据块，即由业务节点发送至协调节点。

[52]在数据库系统中的协调节点获取到数据块之后，则需要对该数据块进行存储。如图 3 所示，图 3 是本说明书实施例提供的应用于数据库系统中的一种数据存储方法的流程示意图，该流程具体包括如下步骤：

[53]S301，协调节点获取已经生成的数据块，根据所述数据块的块哈希值确定所述数据块所对应的数据节点，将所述数据块分配至相应的数据节点，建立所述数据块和数据节点的路由信息，保存所述路由信息和数据块的块头信息。

[54]在数据库系统中，一般存在多个数据节点。为此，协调节点首先需要确定一个数据块应该分配至哪一个数据节点。具体而言，可以根据数据块的哈希值进行分配。

[55]如前所述，数据块的哈希值可以根据父哈希和自身数据记录的哈希联合计算得到的，并存储在块头中。哈希值（hash values）是使用哈希函数（hash function）计算得到的值，支持的算法包括：MACTripleDES、MD5、RIPEMD160、SHA1、SHA256、SHA384、SHA512 等等，总之，一个数据块的块哈希值是一段较短的字符串，可以唯一的标识该数据块，数据块中任何内容的些微改动都会造成数据块哈希值的有很大变化。

[56]而数据节点一般而言个数是固定的，每个数据节点可以有一个相应的编号。因此，可以将哈希值转换为对应的数值，并对数据节点的数量进行取模计算，因此，可以根据取模的结果确定所述数据块所对应的数据节点。

[57]例如，一个数据块的块哈希值进行数值转换后为 100110120，数据节点共有 10 个，编号分别从 0 至 9，则可知块哈希值对于取模的结果为 0，则可以确定 0 号树节点为该块哈希值所对应的数据节点，可以将该数据块发送至 0 号数据节点进行存储。

[58]由于数据块的块哈希值一般有几百位（位数基于哈希算法确定），因此，还可以从块哈希值中选取指定的若干位（例如，最后 3 位）进行数值转换，以进行取模运算从而确定该数据块所对应的数据节点，从而可以降低计算量。

[59]又例如，还可以将所有的数据节点排列在收尾相接的哈希环上，例如，从 0 至 2^32 大小的哈希环上，而每个节点可以根据自身的地址或者设备标识所对应的哈希值被定位至哈希环上的某个点。每个块哈希值可以基于同样的原理被被定位至哈希环上的某个位置，从而可以顺时针或者逆时针时间的找到最先遇到的数据节点为该块哈希值所对应的数据节点。

[60]在确定了一个数据块所对应的数据节点之后，即可以建立一条关于该数据块的路由信息，并写入协调节点中的路由表。具体而言，一个路由表可以包含有数据块块高、数据块的块哈希、数据块对应的数据节点编号等等信息，并且存储于本地。

[61]此外，除了保存所述路由信息外，协调节点中还应保存每一数据块的块头信息。

[62]S303，所述数据节点接收协调节点所发送的数据块，并存储。

[63]通过本说明书实施例所提供的方案，根据数据块的块哈希建立数据块和数据节点的路由关系，对块链式的账本以数据块的粒度进行分布式存储，并且将块头信息等元数据保存在协调节点中，从而可以降低单一节点设备的存储压力，并且，有利于查询、验证

等操作多进程进行，提高效率更为便利。

[64]例如，假设数据节点有 N 个，以及，数据块在数据节点上分布大致均匀。则基于本说明书实施例所提供的方案，需要对账本进行全量验证时，可以将对于数据块的内部验证分配到 N 个数据节点上进行，这相比于常规的从头到尾的串行验证，效率可以提高 N 倍。

[65]当目标数据节点中，时数据块标识可以以块头中所包含的块高或者数据块的块哈希作为标识。在一种实施例中，协调节点还可以仅发送数据块的块体和标识至数据节点中，此时，在数据节点则可以只需要存储块体、块体标识和用于验证的信息即可。数据块标识可以有多种，例如，数据块的块高，和/或，数据块的块哈希等等。在这种方式下协调节点中的路由信息中包含有块体的标识和数据节点编号，上述方式可以节约协调节点的数据传输开销和数据节点的存储空间。用于验证的信息则是指用于验证该数据块完整性的信息，具体可以包括数据块的哈希值以及父数据块的哈希值。

[66]在上述存储方式的基础上，当接收到用户发起的验证指令时。数据库系统则可以进行并行式的验证。如图 3 所示，图 3 为本说明书实施例所提供的数据验证方法的流程示意图，应用于中心化存储块链式账本的数据库系统中，所述数据库系统包括协调节点和数据节点，包括:

[67]S301，协调节点接收第一验证指令，确定待验证的目标账本，根据协调节点中存储的块头信息，对所述目标账本中数据块的块头执行块头完整性验证，所述目标账本包括部分账本或者全量账本。

[68]此处的第一验证指令可以是一个用户输入的操作指令。例如，VERIFY('khash', &v, -1)，其中的'khash'即为用户输入的数据块的哈希值，系统可以根据该哈希值确定出对应的数据块，从而可以将从该数据块至“-1 数据块”（即，初始数据块）之间的所有数据块作为目标账本。又例如，用户可以直接输入指定的数据块的块高: VERIFY（1，1000），从而将前 1000 个数据块作为目标账本。又例如，用户可以输入指定的时间点 VERIFY（T1，T2），从而可以对 T1 至 T2 之间所生成的数据块作为目标账本进行验证，以及，目标账本还可以是当前的全量账本。

[69]此处的验证指的是完整性验证。如前所述，在本说明书实施例中，由于一个数据块的哈希值时基于前一数据块的哈希值和自身数据块的数据记录所按确定的哈希值共同得到，对于数据记录的任意改动都会造成数据块的哈希值的变动。

[70]因此，用户可以随时发起对于数据块是否完整或者正确的完整性验证：验证存储于块头中的该数据块的块哈希是否正确。具体方式即为：从目标账本的第一个数据块开始，按照生成顺序，根据前一数据块的块哈希和该数据块的数据记录所对应的默克尔树的根哈希，生成本数据块的块哈希，并且与预先保存的块头信息中的数据块的块哈希进行对比即可。这种粒度的验证方式下，由于只需要块头的信息，因此可以只在存储有块头信息的协调节点中进行就可以。

[71]S303，若块头完整性验证通过，根据协调节点中存储的数据块和数据节点的路由信息，确定待验证的目标账本中每个数据块对应的目标数据节点。

[72]如果基于块头信息的验证都失败，那么，显然此时无需进一步的验证了，返回完整性验证失败即可。

[73]在块头完整性验证通过以后，则可以进一步的进行块体内的完整性验证。由于在上述存储方式中，具体的数据块的信息并不是存储在协调节点中，而是分布式的存储在数据节点中。因此，需要将进一步的验证工作进行分配。具体的，由于目标账本中包含有多个数据块，每个数据块在存储的时候已经建立相关的路由信息，因此，可以分别确定每个数据块所对应的目标数据节点。对于任一数据块而言，目标数据节点指的是存储该数据块的数据节点。

[74]协调节点基于预先预存的路由信息，可以得知每个数据块存储在哪个数据节点上，由此，可以分别确定出多个目标数据节点，所述多个目标数据节点中存储了目标账本中的全体数据块。

[75]S305，发送第二验证指令至目标数据节点，其中，所述第二验证指令中包含数据块标识。

[76]进而，针对任一已经被确定的目标数据节点，协调节点可以生成相应的第二验证指令并发送，每个第二验证指令中包含有数据块标识，其中，上述数据块标识所对应的数据块应当被存储在该目标数据节点中。数据块标识可以是块高或者数据块的块哈希，其应当与数据节点中存储的数据块标识的类型相同。

[77]在上述过程中，由于目标数据节点存在多个，每个数据节点均会接收到一个第二验证指令。

[78]S307，数据节点接收第二验证指令，对数据块标识对应的数据块执行块体完整性验证，生成验证结果，并返回验证结果至协调节点。

[79]任一数据节点在接收到第二验证指令后，即可以根据数据块标识确定出需要在自身进行验证的数据块。具体的验证方式即为获取每一条数据记录的哈希值，计算得到该该数据块内的数据记录的默克尔树的根哈希值，进而根据之前存储的父哈希值计算得到该数据块的哈希值，并与之前存储的该数据块的哈希值进行对比，一致则验证成功，不一致则验证失败，并且返回验证结果至协调节点。

[80]S309，协调节点接收验证结果，并确定所述目标账本的完整性。

[81]验证结果需要全部都是验证成功，协调节点才可确定账本完整。其中若有任一结果是验证失败，则确定账本不完整。

[82]通过本说明书实施例所提供的方案，当需要到对块链式的账本进行验证时，可以首先只在协调节点中对块头进行完整性验证，验证通过之后，再分发进一步的第二验证指令至各数据节点中，让各数据节点并行执行数据块内部的验证，从而可以大幅提高验证效率。

[83]在一个实施例中，协调节点在进行块头的完整性验证时，还可以基于时间公正机构所生成授时证书进行。授时证书可以基于如下方式预先生成：协调节点确定需要进行授时认证的目标账本，所述目标账本中至少包含一个数据块，或者多个块高连续的数据块；按照所述目标账本中数据块的块高的顺序，生成对应于所述目标账本的默克尔树，基于各数据块的块哈希确定所述默克尔树的根哈希；将所述默克尔树的根哈希和数据块的相关信息发送至时间公正机构，其中，所述数据块的相关信息包括起始块高、结束块高或者数据块的数量；接收时间公正机构所返回的对应于所述目标账本的包含可信时间戳和时间公正机构签名的的授时证书。在一个授时证书中包括对应的部分账本的起点数据块高、终点数据块高、可信时间戳和所述部分账本的根哈希。

[84]换言之，一个授时证书是用于确认一段账本的生成时间在时间公正机构所给出的时间戳之前。时间公正机构可以是国家授时中心，或者国家授时中心所授权的相关授时机构。

[85]具体而言，在第一验证指令可以包含有一个时间点，或者，由两个时间点所确定的时间区间。协调节点可以根据授时证书中的可信时间戳与第一验证指令中的时间点进行匹配。例如，在第一验证指令中包含有一个时间点时，对应的授时证书可以是可信时间戳与该时间点间隔最小的授时证书；在第一验证指令中包含有两个时间点所确定的时间区间时，对应的授时证书可以是可信时间戳落入该区间的所有授时证书。

[86]基于授时证书的块头完整性验证时，验证的数据块的范围由授时证书中所包含的起始块高和结束块高确定。验证的方式即为构建从起始块高至结束块高的默克尔树，并计算根哈希，与授时证书中的根哈希进行对比即可。

[87]当授时证书存在多个时，可以按照授时证书中的可信时间戳的先后顺序依次对授时证书所对应的部分账本进行块头完整性验证。

[88]在另一个实施例中，协调节点接收到对于账本的全量验证指令。此时，全量验证指令中无需包含时间点，协调节点可以基于全部的授时证书，对全量账本进行块头完整性验证。

[89]需要说明的是，由于授时证书也是存储在协调节点中，因此，基于授时证书的块头完整性验证也可以只在协调节点中进行，无需调用数据节点。

[90]在一个实施例中，协调节点在接收数据节点所返回的对于数据块的验证结果之前，可以生成一个在协调节点中生成一个完整性数组，用于记录数据节点对于所述目标账本中数据块的验证结果。而数据节点在生成验证结果时，可以返回用于表征失败或者成功的特征值。例如，验证成功返回 1，验证失败返回 0。从而完整性数组中的元素的取值要么为 1，要么为 0。当完整性数组中存在任一元素取值为 0 时，则协调节点即可确认验证失败，而当完整性数组中所有元素取值为 1 时，协调节点才确认验证成功，通过完整性数组记录每个数据块的验证状态可以更便利的统计验证结果。

[91]对应的，本说明书实施例还提供一种数据验证系统，应用于中心化存储块链式账本的数据库系统中，所述数据库系统包括协调节点和数据节点，

[92]协调节点接收第一验证指令，确定待验证的目标账本，根据协调节点中存储的块头信息，对所述目标账本中数据块的块头执行块头完整性验证，所述目标账本包括部分账本或者全量账本；若块头完整性验证通过，根据协调节点中存储的数据块和数据节点的路由信息，确定待验证的目标账本中每个数据块对应的目标数据节点，发送第二验证指令至目标数据节点，其中，所述第二验证指令中包含数据块标识；

[93]数据节点接收第二验证指令，对数据块标识对应的数据块执行块体完整性验证，生成验证结果，并返回验证结果至协调节点；

[94]协调节点接收验证结果，并确定所述目标账本的完整性；

[95]其中，在所述块链式账本中，数据块包含用于存储元数据的块头，和，用于存储数据记录的块体；除初始数据块以外，每一数据块中包含至少一条数据记录，每一数据块

中包含由前一数据块的哈希值和自身所包含的数据记录确定的自身数据块的块哈希值，数据块的块高基于成块时间的先后顺序单调递增。

[96]进一步地，在所述数据库系统中，数据块通过如下方式预先存储：协调节点获取已经生成的数据块，根据所述数据块的块哈希值确定所述数据块所对应的数据节点，将所述数据块分配至相应的数据节点，建立所述数据块和数据节点的路由信息，保存所述路由信息和数据块的块头信息；所述数据节点接收协调节点所发送的数据块，并存储。

[97]进一步地，在所述数据库系统中，协调节点获取所述数据块中的块头和块体，将所述块体分配至相应的数据节点；相应的，协调节点建立所述块体和数据节点的路由信息；相应的，所述数据节点接收协调节点所发送的块体。

[98]进一步地，在所述数据库系统中，数据块通过如下方式预先生成：接收待存储的数据记录，确定各数据记录的哈希值；当达到预设的成块条件时，确定待写入数据块中的各数据记录，生成包含数据块的哈希值和数据记录的第 N 个数据块，具体包括：

[99]当 N=1 时，初始数据块的哈希值和块高基于预设方式给定；

[100] 当 N>1 时，根据待写入数据块中的各数据记录和第 N－1 个数据块的哈希值确定第 N 个数据块的哈希值，生成包含第 N 个数据块的哈希值、各数据记录和数据块的成块时间的第 N 个数据块，其中，数据块的块高基于成块时间的先后顺序单调递增。

[101] 进一步地，在所述数据库系统中，协调节点接收第一验证指令中所包含的时间点，获取所述时间点所对应的授时证书，将所述授时证书所对应的部分账本确定为待验证的目标账本，其中，所述授时证书中包括所述对应的部分账本的起点数据块高、终点数据块高、可信时间戳和所述部分账本的根哈希；相应的，协调节点根据所述授时证书和所述存储的块头信息，对所述部分账本执行块头完整性验证。

[102] 进一步地，在所述数据库系统中，在协调节点接收验证结果之前，协调节点生成用于记录所述目标账本中数据块的验证结果的完整性数组，其中，所述完整性数组中每一个元素对应于一个数据块；相应的，数据节点生成验证结果，并返回验证结果至协调节点，包括：数据节点生成表征验证失败或者成功的特征值至协调节点；相应的，协调节点接收验证结果，并确定所述目标账本的完整性，包括：当所述完整性数组中任一元素的取值为表征验证失败的特征值时，确定目标账本不完整。

[103] 对应的，本说明书实施例还提供一种数据验证方法，应用于中心化存储块链式账本的数据库系统中的协调节点中，如图 4 所示，图 4 为本说明书实施例所提供的应用

于协调节点中的数据验证方法的流程示意图，包括：

[104] S401，接收第一验证指令，确定待验证的目标账本，根据协调节点中存储的块头信息，对所述目标账本中数据块的块头执行块头完整性验证，所述目标账本包括部分账本或者全量账本；

[105] S403，若块头完整性验证通过，根据协调节点中存储的数据块和数据节点的路由信息，确定待验证的目标账本中每个数据块对应的目标数据节点，

[106] S405，发送第二验证指令至目标数据节点，其中，所述第二验证指令中包含数据块标识；

[107] S407，接收目标数据节点所返回的对于数据块的验证结果，根据所述验证结果确定目标账本的完整性；

[108] 其中，在所述块链式账本中，数据块包含用于存储元数据的块头，和，用于存储数据记录的块体；除初始数据块以外，每一数据块中包含至少一条数据记录，每一数据块中包含由前一数据块的哈希值和自身所包含的数据记录确定的自身数据块的块哈希值，数据块的块高基于成块时间的先后顺序单调递增。

[109] 对应的，本说明书实施例还提供一种数据验证装置，应用于中心化存储块链式账本的数据库系统中的协调节点中，如图 5 所示，图 5 为本说明书实施例所提供的应用于协调节点中的数据验证装置的结构示意图，包括：

[110] 块头验证模块 501，接收第一验证指令，确定待验证的目标账本，根据协调节点中存储的块头信息，对所述目标账本中数据块的块头执行块头完整性验证，所述目标账本包括部分账本或者全量账本；

[111] 确定模块 503，若块头完整性验证通过，根据协调节点中存储的数据块和数据节点的路由信息，确定待验证的目标账本中每个数据块对应的目标数据节点，

[112] 发送模块 505，发送第二验证指令至目标数据节点，其中，所述第二验证指令中包含数据块标识；

[113] 接收模块 507，接收目标数据节点所返回的对于数据块的验证结果，根据所述验证结果确定目标账本的完整性。

[114] 其中，在所述块链式账本中，数据块包含用于存储元数据的块头，和，用于存储数据记录的块体；除初始数据块以外，每一数据块中包含至少一条数据记录，每一数

据块中包含由前一数据块的哈希值和自身所包含的数据记录确定的自身数据块的块哈希值，数据块的块高基于成块时间的先后顺序单调递增。

[115] 本说明书实施例还提供一种计算机设备，其至少包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其中，处理器执行所述程序时实现图 4 所示的数据验证方法。

[116] 图 6 示出了本说明书实施例所提供的一种更为具体的计算设备硬件结构示意图，该设备可以包括：处理器 1010、存储器 1020、输入/输出接口 1030、通信接口 1040 和总线 1050。其中处理器 1010、存储器 1020、输入/输出接口 1030 和通信接口 1040 通过总线 1050 实现彼此之间在设备内部的通信连接。

[117] 处理器 1010 可以采用通用的 CPU（Central Processing Unit，中央处理器）、微处理器、应用专用集成电路（Application Specific Integrated Circuit，ASIC）、或者一个或多个集成电路等方式实现，用于执行相关程序，以实现本说明书实施例所提供的技术方案。

[118] 存储器 1020 可以采用 ROM（Read Only Memory，只读存储器）、RAM（Random Access Memory，随机存取存储器）、静态存储设备，动态存储设备等形式实现。存储器 1020 可以存储操作系统和其他应用程序，在通过软件或者固件来实现本说明书实施例所提供的技术方案时，相关的程序代码保存在存储器 1020 中，并由处理器 1010 来调用执行。

[119] 输入/输出接口 1030 用于连接输入/输出模块，以实现信息输入及输出。输入输出/模块可以作为组件配置在设备中（图中未示出），也可以外接于设备以提供相应功能。其中输入设备可以包括键盘、鼠标、触摸屏、麦克风、各类传感器等，输出设备可以包括显示器、扬声器、振动器、指示灯等。

[120] 通信接口 1040 用于连接通信模块（图中未示出），以实现本设备与其他设备的通信交互。其中通信模块可以通过有线方式（例如 USB、网线等）实现通信，也可以通过无线方式（例如移动网络、WIFI、蓝牙等）实现通信。

[121] 总线 1050 包括一通路，在设备的各个组件（例如处理器 1010、存储器 1020、输入/输出接口 1030 和通信接口 1040）之间传输信息。

[122] 需要说明的是，尽管上述设备仅示出了处理器 1010、存储器 1020、输入/输出接口 1030、通信接口 1040 以及总线 1050，但是在具体实施过程中，该设备还可以包括实

现正常运行所必需的其他组件。此外，本领域的技术人员可以理解的是，上述设备中也可以仅包含实现本说明书实施例方案所必需的组件，而不必包含图中所示的全部组件。

[123] 本说明书实施例还提供一种计算机可读存储介质，其上存储有计算机程序，该程序被处理器执行时实现图 4 所示的数据验证方法。

[124] 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存（PRAM）、静态随机存取存储器（SRAM）、动态随机存取存储器（DRAM）、其他类型的随机存取存储器（RAM）、只读存储器（ROM）、电可擦除可编程只读存储器（EEPROM）、快闪记忆体或其他内存技术、只读光盘只读存储器（CD-ROM）、数字多功能光盘（DVD）或其他光学存储、磁盒式磁带，磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括暂存电脑可读媒体（transitory media），如调制的数据信号和载波。

[125] 通过以上的实施方式的描述可知，本领域的技术人员可以清楚地了解到本说明书实施例可借助软件加必需的通用硬件平台的方式来实现。基于这样的理解，本说明书实施例的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）执行本说明书实施例各个实施例或者实施例的某些部分所述的方法。

[126] 上述实施例阐明的系统、方法、模块或单元，具体可以由计算机芯片或实体实现，或者由具有某种功能的产品来实现。一种典型的实现设备为计算机，计算机的具体形式可以是个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件收发设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任意几种设备的组合。

[127] 本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于方法实施例而言，由于其基本相似于方法实施例，所以描述得比较简单，相关之处参见方法实施例的部分说明即可。以上所描述的方法实施例仅仅是示意性的，其中所述作为分离部件说明的模块可以是或者也可以不是物理上分开的，在实施本说明书实施例方案时可以把各模块的功能在同一个或多个软件和/或硬件中实现。也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劳动的情况下，即可以理解并实施。

[128] 以上所述仅是本说明书实施例的具体实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本说明书实施例原理的前提下，还可以做出若干改进和润饰，这些改进和润饰也应视为本说明书实施例的保护范围。

权利要求书

1、一种数据验证方法，应用于中心化存储块链式账本的数据库系统中，所述数据库系统包括协调节点和数据节点，所述方法包括：

协调节点接收第一验证指令，确定待验证的目标账本，根据协调节点中存储的块头信息，对所述目标账本中数据块的块头执行块头完整性验证，所述目标账本包括部分账本或者全量账本；

若块头完整性验证通过，根据协调节点中存储的数据块和数据节点的路由信息，确定待验证的目标账本中每个数据块对应的目标数据节点；

发送第二验证指令至目标数据节点，其中，所述第二验证指令中包含数据块标识；

数据节点接收第二验证指令，对数据块标识对应的数据块执行块体完整性验证，生成验证结果，并返回验证结果至协调节点；

协调节点接收验证结果，并确定所述目标账本的完整性；

其中，在所述块链式账本中，数据块包含用于存储元数据的块头，和，用于存储数据记录的块体；除初始数据块以外，每一数据块中包含至少一条数据记录，每一数据块中包含由前一数据块的哈希值和自身所包含的数据记录确定的自身数据块的块哈希值，数据块的块高基于成块时间的先后顺序单调递增。

2、如权利要求 1 所述的方法，在所述数据库系统中，数据块通过如下方式预先存储：

协调节点获取已经生成的数据块，根据所述数据块的块哈希值确定所述数据块所对应的数据节点，将所述数据块分配至相应的数据节点，建立所述数据块和数据节点的路由信息，保存所述路由信息和数据块的块头信息；

所述数据节点接收协调节点所发送的数据块，并存储。

3、如权利要求 2 所述的方法，协调节点将所述数据块分配至相应的数据节点，包括：

协调节点获取所述数据块中的块头和块体，将所述块体分配至相应的数据节点；

相应的，建立所述数据块和数据节点的路由信息，包括：建立所述块体和数据节点的路由信息；

相应的，所述数据节点接收协调节点所发送的数据块，包括：所述数据节点接收协调节点所发送的块体。

4、如权利要求 2 所述的方法，在所述数据库系统中，数据块通过如下方式预先生成：

接收待存储的数据记录，确定各数据记录的哈希值；

当达到预设的成块条件时，确定待写入数据块中的各数据记录，生成包含数据块的哈希值和数据记录的第 N 个数据块，具体包括：

当 N=1 时，初始数据块的哈希值和块高基于预设方式给定；

当 N>1 时，根据待写入数据块中的各数据记录和第 N－1 个数据块的哈希值确定第 N 个数据块的哈希值，生成包含第 N 个数据块的哈希值、各数据记录和数据块的成块时间的第 N 个数据块，其中，数据块的块高基于成块时间的先后顺序单调递增。

5、如权利要求 1 所述的方法，协调节点接收第一验证指令，确定待验证的目标账本，包括：

协调节点接收第一验证指令中所包含的时间点，获取所述时间点所对应的授时证书，将所述授时证书所对应的部分账本确定为待验证的目标账本，其中，所述授时证书中包括所述对应的部分账本的起点数据块高、终点数据块高、可信时间戳和所述部分账本的根哈希；

相应的，根据协调节点中存储的块头信息，对所述目标账本中数据块的块头执行块头完整性验证，包括：根据所述授时证书和所述存储的块头信息，对所述部分账本执行块头完整性验证。

6、如权利要求 1 所述的方法，在协调节点接收验证结果之前，所述方法还包括：

协调节点生成用于记录所述目标账本中数据块的验证结果的完整性数组，其中，所述完整性数组中每一个元素对应于一个数据块；

相应的，数据节点生成验证结果，并返回验证结果至协调节点，包括：数据节点生成表征验证失败或者成功的特征值至协调节点；

相应的，协调节点接收验证结果，并确定所述目标账本的完整性，包括：当所述完整性数组中任一元素的取值为表征验证失败的特征值时，确定目标账本不完整。

7、一种数据验证系统，应用于中心化存储块链式账本的数据库系统中，所述数据库系统包括协调节点和数据节点，

协调节点接收第一验证指令，确定待验证的目标账本，根据协调节点中存储的块头信息，对所述目标账本中数据块的块头执行块头完整性验证，所述目标账本包括部分账本或者全量账本；

若块头完整性验证通过，根据协调节点中存储的数据块和数据节点的路由信息，确定待验证的目标账本中每个数据块对应的目标数据节点，

发送第二验证指令至目标数据节点，其中，所述第二验证指令中包含数据块标识；

数据节点接收第二验证指令，对数据块标识对应的数据块执行块体完整性验证，生成验证结果，并返回验证结果至协调节点；

协调节点接收验证结果，并确定所述目标账本的完整性；

其中，在所述块链式账本中，数据块包含用于存储元数据的块头，和，用于存储数据记录的块体；除初始数据块以外，每一数据块中包含至少一条数据记录，每一数据块中包含由前一数据块的哈希值和自身所包含的数据记录确定的自身数据块的块哈希值，数据块的块高基于成块时间的先后顺序单调递增。

8、如权利要求 7 所述的系统，在所述数据库系统中，数据块通过如下方式预先存储：

协调节点获取已经生成的数据块，根据所述数据块的块哈希值确定所述数据块所对应的数据节点，将所述数据块分配至相应的数据节点，建立所述数据块和数据节点的路由信息，保存所述路由信息和数据块的块头信息；

所述数据节点接收协调节点所发送的数据块，并存储。

9、如权利要求 8 所述的系统，

协调节点获取所述数据块中的块头和块体，将所述块体分配至相应的数据节点；相应的，协调节点建立所述块体和数据节点的路由信息；相应的，所述数据节点接收协调节点所发送的块体。

10、如权利要求 8 所述的系统，在所述数据库系统中，数据块通过如下方式预先生成：接收待存储的数据记录，确定各数据记录的哈希值；当达到预设的成块条件时，确定待写入数据块中的各数据记录，生成包含数据块的哈希值和数据记录的第 N 个数据块，具体包括：

当 N=1 时，初始数据块的哈希值和块高基于预设方式给定；

当 N>1 时，根据待写入数据块中的各数据记录和第 N－1 个数据块的哈希值确定第 N 个数据块的哈希值，生成包含第 N 个数据块的哈希值、各数据记录和数据块的成块时间的第 N 个数据块，其中，数据块的块高基于成块时间的先后顺序单调递增。

11、如权利要求 7 所述的系统，

协调节点接收第一验证指令中所包含的时间点，获取所述时间点所对应的授时证书，将所述授时证书所对应的部分账本确定为待验证的目标账本，其中，所述授时证书中包括所述对应的部分账本的起点数据块高、终点数据块高、可信时间戳和所述部分账本的根哈希；

相应的，协调节点根据所述授时证书和所述存储的块头信息，对所述部分账本执行

块头完整性验证。

12、如权利要求 7 所述的系统，在协调节点接收验证结果之前，

协调节点生成用于记录所述目标账本中数据块的验证结果的完整性数组，其中，所述完整性数组中每一个元素对应于一个数据块；

相应的，数据节点生成验证结果，并返回验证结果至协调节点，包括：数据节点生成表征验证失败或者成功的特征值至协调节点；

相应的，协调节点接收验证结果，并确定所述目标账本的完整性，包括：当所述完整性数组中任一元素的取值为表征验证失败的特征值时，确定目标账本不完整。

13、一种数据验证方法，应用于中心化存储块链式账本的数据库系统中的协调节点中，所述方法包括：

接收第一验证指令，确定待验证的目标账本，根据协调节点中存储的块头信息，对所述目标账本中数据块的块头执行块头完整性验证，所述目标账本包括部分账本或者全量账本；

若块头完整性验证通过，根据协调节点中存储的数据块和数据节点的路由信息，确定待验证的目标账本中每个数据块对应的目标数据节点，

发送第二验证指令至目标数据节点，其中，所述第二验证指令中包含数据块标识；

接收目标数据节点所返回的对于数据块的验证结果，根据所述验证结果确定目标账本的完整性。

14、一种数据验证装置，应用于中心化存储块链式账本的数据库系统中的协调节点中，所述装置包括：

块头验证模块，接收第一验证指令，确定待验证的目标账本，根据协调节点中存储的块头信息，对所述目标账本中数据块的块头执行块头完整性验证，所述目标账本包括部分账本或者全量账本；

确定模块，若块头完整性验证通过，根据协调节点中存储的数据块和数据节点的路由信息，确定待验证的目标账本中每个数据块对应的目标数据节点，

发送模块，发送第二验证指令至目标数据节点，其中，所述第二验证指令中包含数据块标识；

接收模块，接收目标数据节点所返回的对于数据块的验证结果，根据所述验证结果确定目标账本的完整性。

15、一种计算机设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其中，所述处理器执行所述程序时实现如权利要求 13 所述的方法。

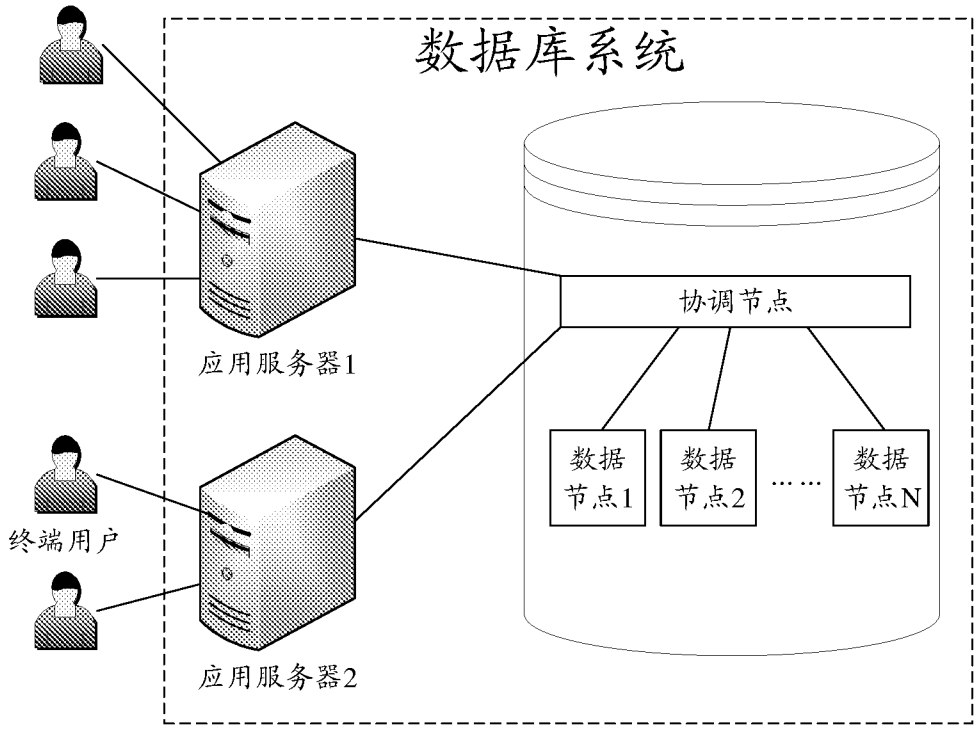


图 1

字段名称	字段类型	字段说明
Hash	h256	数据块的哈希值
Version	Uint32_t	版本号
Number	Uint64_t	块高
Parent_hash	h256	父数据块的哈希值
Tx_root	h256	块体中的交易的默克尔树根哈希
Time_stamp	Uint64_t	时间戳

图 2


协调节点接收第一验证指令，确定待验证的目标账本，根据协调节点中存储的块头信息，对所述目标账本中数据块的块头执行块头完整性验证
301
若块头完整性验证通过，根据协调节点中存储的数据块和数据节点的路由信息，确定待验证的目标账本中每个数据块对应的目标数据节点
303
发送第二验证指令至目标数据节点，其中，所述第二验证指令中包含数据块标识
305
数据节点接收第二验证指令，对数据块标识对应的数据块执行块体完整性验证，生成验证结果，并返回验证结果至协调节点
307
协调节点接收验证结果，并确定所述目标账本的完整性
309

图 3

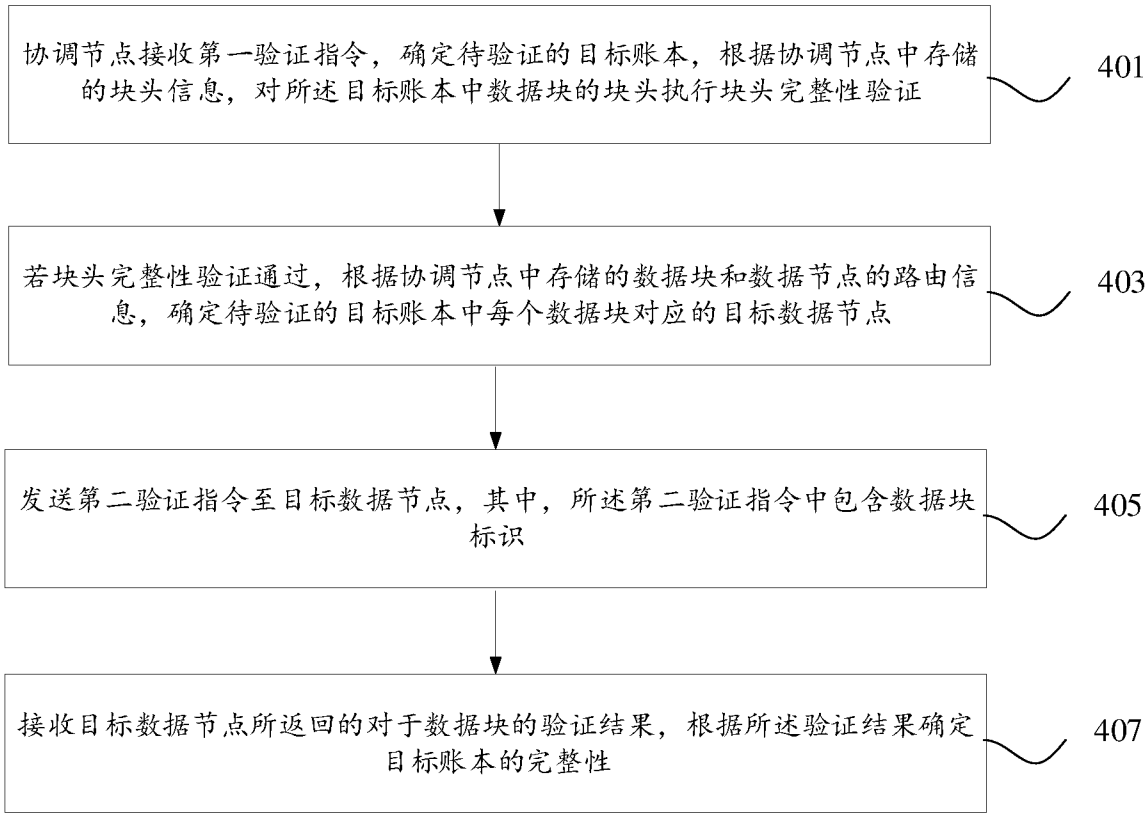

协调节点接收第一验证指令，确定待验证的目标账本，根据协调节点中存储的块头信息，对所述目标账本中数据块的块头执行块头完整性验证
401
若块头完整性验证通过，根据协调节点中存储的数据块和数据节点的路由信息，确定待验证的目标账本中每个数据块对应的目标数据节点
403
发送第二验证指令至目标数据节点，其中，所述第二验证指令中包含数据块标识
405
接收目标数据节点所返回的对于数据块的验证结果，根据所述验证结果确定目标账本的完整性
407

图 4

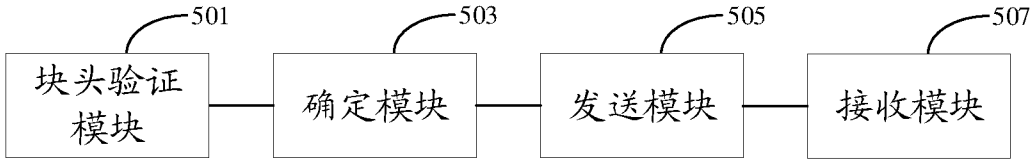

501
503
505
507
块头验证模块
确定模块
发送模块
接收模块

图 5

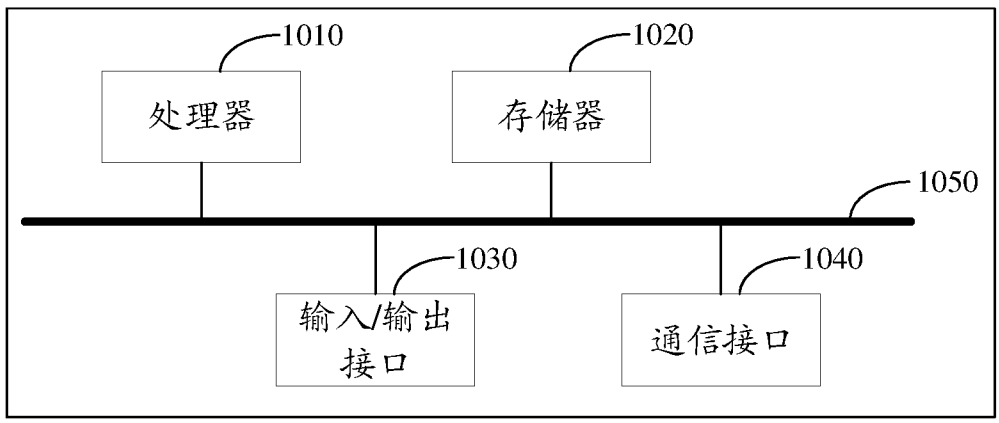

1010
1020
处理器
存储器
1050
1030
1040
输入/输出接口
通信接口

图 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2020/071219

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/64(2013.01)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)

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, WPI, EPODOC, IEEE, CNKI: 区块, 验证, 块头, 完整性, 节点, 哈希, 标识, 索引, 分发, 分布, blockchain, head, validate, verify, hash, index, distribute

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110147685 A (ALIBABA GROUP HOLDING LIMITED) 20 August 2019 (2019-08-20) claims 1-15	1-15
A	CN 107657438 A (UNION MOBILE PAY CO., LTD.) 02 February 2018 (2018-02-02) description, paragraphs [0148]-[0154]	1-15
A	CN 109242500 A (BAIDU ONLINE NETWORK TECHNOLOGY BEIJING CO., LTD.) 18 January 2019 (2019-01-18) entire document	1-15
A	US 2019036932 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 31 January 2019 (2019-01-31) entire document	1-15

☐ 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
27 March 2020	**10 April 2020**
Name and mailing address of the ISA/CN **China National Intellectual Property Administration (ISA/CN)** **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China** Facsimile No. **(86-10)62019451**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2020/071219

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	110147685	A	20 August 2019	None			
CN	107657438	A	02 February 2018	None			
CN	109242500	A	18 January 2019	None			
US	2019036932	A1	31 January 2019	US	2020045051	A1	06 February 2020
				WO	2019020616	A1	31 January 2019

国际检索报告

国际申请号
PCT/CN2020/071219

A. 主题的分类

G06F 21/64(2013.01)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)

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, WPI, EPODOC, IEEE, CNKI: 区块, 验证, 块头, 完整性, 节点, 哈希, 标识, 索引, 分发, 分布, blockchain, head, validate, verify, hash, index, distribute

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 110147685 A (阿里巴巴集团控股有限公司) 2019年 8月 20日 (2019-08-20) 权利要求1-15	1-15
A	CN 107657438 A (联动优势科技有限公司) 2018年 2月 2日 (2018-02-02) 说明书第[0148]-[0154]段	1-15
A	CN 109242500 A (百度在线网络技术北京有限公司) 2019年 1月 18日 (2019-01-18) 全文	1-15
A	US 2019036932 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 2019年 1月 31日 (2019-01-31) 全文	1-15

☐ 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 3月 27日	2020年 4月 10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 任兴超 电话号码 86-(10)-53961375

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2020/071219

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	110147685	A	2019年 8月 20日	无			
CN	107657438	A	2018年 2月 2日	无			
CN	109242500	A	2019年 1月 18日	无			
US	2019036932	A1	2019年 1月 31日	US	2020045051	A1	2020年 2月 6日
				WO	2019020616	A1	2019年 1月 31日