(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 11 月 26 日 (26.11.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/233149 A1

(51) 国际专利分类号:
H04L 9/32 (2006.01)

(21) 国际申请号: PCT/CN2020/071687

(22) 国际申请日: 2020 年 1 月 13 日 (13.01.2020)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910436532.2 2019年5月23日 (23.05.2019) 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, Grand 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:** METHOD, APPARATUS AND DEVICE FOR TIMING AUTHENTICATION IN BLOCKCHAIN ACCOUNT BOOK

(54) 发明名称: 一种块链式账本中的授时认证方法、装置及设备

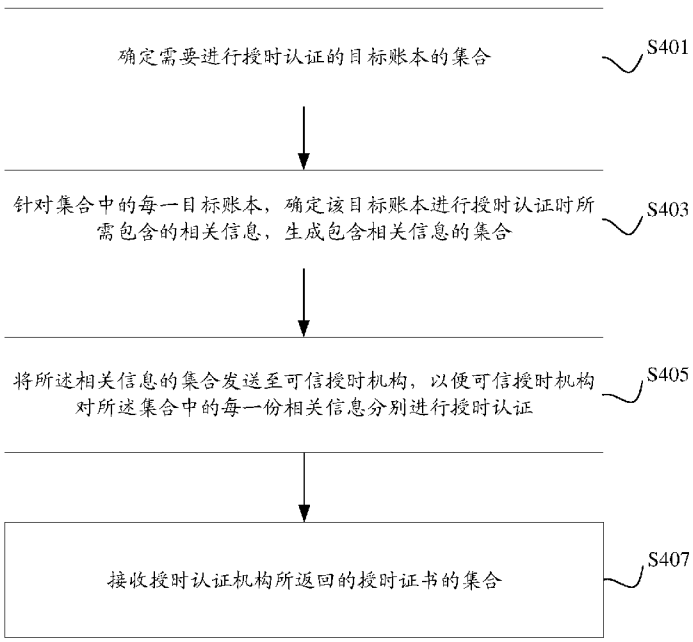


图 4

(57) **Abstract:** Disclosed are a method, apparatus and device for timing authentication in a blockchain account book. According to the solution provided in the embodiments of the specification, when timing authentication is performed, batch application can be performed on target account books on which timing authentication needs to be performed, so as to prevent each account book from independently applying for timing authentication; in addition, when performing batch timing authentication, personalized timing authentication can also be performed according to a time granularity selected by a user.

WO 2020/233149 A1

[见续页]

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))。

(57) 摘要：公开了一种块链式账本中的授时认证方法、装置及设备。通过本说明书实施例所提供的方案，在进行授时认证时，可以对需要进行授时认证的目标账本进行批量申请，从而避免每个账本单独申请授时认证；此外，在批量授时认证时，还可以根据用户所选择的时间粒度，进行个性化的授时认证。

一种块链式账本中的授时认证方法、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，尤其涉及一种块链式账本中的授时认证方法、装置及设备。

背景技术

[02] 在块链式的账本中，服务方本身已经难以对数据进行直接修改，但此时，仍然存在用户或者企业与服务方联合作假的可能性。因此，用户有需求需要对自身的账本进行授时认证来防止作假。在账本数量较多时，则需要可以对多个账本进行授时认证。

[03] 基于此，需要一种链式账本中批量进行授时认证的方案。

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对多个账本进行批量授时认证的方法。

[05] 为解决上述技术问题，本申请实施例是这样实现的:

[06] 一种块链式账本中的授时认证方法，应用于通过块链式账本存储数据的中心化的数据库服务端中，所述方法包括:

[07] 确定需要进行授时认证的目标账本的集合，所述集合中包含至少一个目标账本，其中，所述目标账本至少包含一个数据块，或者包含同一账本中多个块高连续的数据块;

[08] 针对集合中的每一目标账本，确定该目标账本进行授时认证时所需包含的相关信息，生成包含相关信息的集合，其中，每一份相关信息对应于一份目标账本，所述相关信息包括该目标账本的标识、起始块高、结束块高、该账目标账本中数据块构成的默克尔树的根哈希;

[09] 将所述相关信息的集合发送至可信授时机构，以便可信授时机构对所述集合中的每一份相关信息分别进行授时认证;

[10] 接收授时认证机构所返回的授时证书的集合，其中，授时证书包含可信时间戳、所述相关信息和可信授时机构数字签名，授时证书、授时证书中包含的相关信息和目标

账本存在一一对应关系。

[11] 对应的，本说明书实施例还提供一种块链式账本中的授时认证装置，应用于通过块链式账本存储数据的中心化的数据库服务端中，所述装置包括：

[12] 目标账本确定模块，确定需要进行授时认证的目标账本的集合，所述集合中包含至少一个目标账本，其中，所述目标账本至少包含一个数据块，或者包含同一账本中多个块高连续的数据块；

[13] 信息集合生成模块，针对集合中的每一目标账本，确定该目标账本进行授时认证时所需包含的相关信息，生成包含相关信息的集合，其中，每一份相关信息对应于一份目标账本，所述相关信息包括该目标账本的标识、起始块高、结束块高、该账目标账本中数据块构成的默克尔树的根哈希；

[14] 发送模块，将所述相关信息的集合发送至可信授时机构，以便可信授时机构对所述集合中的每一份相关信息分别进行授时认证；

[15] 授时证书接收模块，接收授时认证机构所返回的授时证书的集合，其中，授时证书包含可信时间戳、所述相关信息和可信授时机构数字签名，授时证书、授时证书中包含的相关信息和目标账本存在一一对应关系。

[16] 通过本说明书实施例所提供的方案，在进行授时认证时，可以对需要进行授时认证的目标账本进行批量申请，从而避免每个账本单独申请授时认证；此外，在批量授时认证时，还可以根据用户所选择的时间粒度，进行个性化的授时认证。本说明书实施例所提供的方案通过对目标账本进行批量注册，可以提高效率，便于对授时证书的管理。

[17] 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。

[18] 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

[19] 为了更清楚地说明本说明书实施例中的技术方案，下面将对实施例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。

[20] 图 1 当前技术中所涉及的系统架构的示意图；

[21] 图 2 为本说明书实施例所提供的块链式账本中数据块的生成方式的流程示意图;

[22] 图 3 为本说明书实施例所提供的一种伪链的示意图;

[23] 图 4 为本说明书实施例所提供的一种块链式账本中的授时认证方法的流程示意图;

[24] 图 5 为本说明书实施例所提供的一种授时证书的结构示意图;

[25] 图 6 为数据库服务端中对于多份账本的授时证书的示意图;

[26] 图 7 是本说明书实施例提供的一种块链式账本中的授时认证的结构示意图;

[27] 图 8 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

[28] 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。

[29] 首先需要说明的是，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。如图 1 所示，图 1 当前技术中所涉及的系统架构的示意图。

[30] 因此，在本说明书实施例中，当用户是应用服务器时，数据库服务提供方可以是图 1 中所示的数据库服务器；而在用户是客户端个人用户时，数据库服务提供方也可以是由应用服务器和数据库服务器构成的服务端整体。但无论在那种情形下，对于数据的存储都是在数据库服务提供方完成，而对于数据的操作（包括增删改查等等）也是基于用户的指令在数据库服务提供方进行，用户数据以及对数据的操作结果均存储在数据库服务提供方，用户本地以及其它设备上不存储数据。换言之，本说明书中的数据库服务提供方是以中心化的形式提供数据服务。

[31] 在本说明书实施例所涉及中心化的数据库服务端中，数据块可以通过如下方式预先生成，如图 2 所示，图 2 为本说明书实施例所提供的块链式账本中数据块的生成方式的流程示意图，包括:

[32] S201，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。

[33] S203，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。

[34] 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。

[35] 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，例如，将数据块的成块时间戳转换为单调递增的大整型数据，以该大整型数据作为数据块的块高。

[36] 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。

[37] 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等等)生成当前快的哈希值。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。

[38] 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或者数据记录的哈希值发起验证，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。

[39] 在上述方式中，仍然有可能用户和服务方联合起来对于部分数据块进行了伪造，重新生成一条相关的伪链，从而形成一个与原账本部分相同的新的账本，以躲避相关的审计和验证。如图 3 所示，图 3 为本说明书实施例所提供的一种伪链的示意图。在生成伪链的过程中，数据块的成块方式和前述的成块方式相同。

[40] 在该示意图中，在账本已经记录了很多数据块之后，业务方认为第 1000 个数据块中的数据记录有问题，因此，为了不暴露该问题，其和数据库服务方联合起来，从第 1000 个数据块开始对数据块进行了替换，重新生成一个新的第 1000 个数据块，接在第 999 个数据块之后，形成一条与原账本部分相同的伪链，以躲避验证和审计，而在外部第三方而言并不能识别出伪链和真链。

[41] 基于此，本说明书实施例还提供一种对于账本进行授时认证的方法，如图 4 所示，图 4 为本说明书实施例所提供的一种块链式账本中的授时认证方法的流程示意图，包括如下步骤：

[42] S401，确定需要进行授时认证的目标账本的集合，所述集合中包含至少一个目标账本，其中，所述目标账本至少包含一个数据块，或者包含同一账本中多个块高连续的数据块。

[43] 如前所述，在所述链式账本中，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哈希值，数据块的块高基于成块时间的先后顺序单调递增。即，数据块是链式存在的。

[44] 对于目标账本的集合中所包含的元素（即任一目标账本），可以基于用户自身的申请，也可以是默认对于服务端中所存在的账本均需要进行授时认证。具体而言，可以通过账本标识来确定目标账本的集合中应该包括哪些目标账本。目标账本的集合中一般包括多个待授时的目标账本。

[45] 在本说明书实施例中，目标账本可以是一个完整的账本。但是，在更多的情形中，目标账本是某一个由账本标识所确定的账本中的一段块高连续的部分账本，或者，是由账本标识所确定的账本中的一个数据块。

[46] 目标账本的具体内容，可以基于用户操作进行指定，例如，用户发起授时指令，指令中包含需要进行授时认证的账本标识、起始块高和块数量，将由账本标识、起始块高和块数量确定的部分账本作为目标账本。

[47] 目标账本也可以是无需用户指定，而是由服务端基于预设的业务逻辑自动进行。例如，从最细粒度上，可以是服务端中的每个账本的每个数据块都去申请授时。在这种方式下，对于一个目标账本而言，部分账本的默克尔树的根哈希即为该数据块的块哈希值，该方式可以最大程度的对各个账本（即各数据块）进行真实性的保护。由于数据块的出块频率较高，这种方式无论对于授时中心，还是对于服务方而言，成本开销都会比较大。

[48] 一种可选的方式为，对于一个账本而言，设置一定的授时预设条件，当满足该授时预设条件时，从该账本中确定出部分账本作为目标账本。对于一个账本而言，在将新生成的数据块都认为是待授时认证的数据块时，所述的授时预设条件可以是：待授时认证的数据块达到数量阈值，或者，距离上一次授时认证的时间间隔已经到达时间阈值。此时，新生成且还未授时认证的数据块组成的部分账本将作为目标账本。

[49] S403，针对集合中的每一目标账本，确定该目标账本进行授时认证时所需包含的相关信息，生成包含相关信息的集合，其中，每一份相关信息对应于一份目标账本，所述相关信息包括该目标账本的标识、起始块高、结束块高、该账目标账本中数据块构成的默克尔树的根哈希；

[50] 首先，对于任一目标账本，可以根据该目标账本中的数据块的顺序以及各数据块的哈希值确定默克尔树的根哈希。具体的根哈希的计算方式即为常规的计算方式，此处不再赘述。在目标账本中只有一个数据块时，数据块的哈希值即为目标账本中的默克尔树的根哈希。

[51] 目标账本的标识、起始块高、结束块高在 S401 中即已经得到确定，此时，对于每一份目标账本，都会对应的生成分目标账本的相关信息。

[52] S405，将所述相关信息的集合发送至可信授时机构，以便可信授时机构对所述集合中的每一份相关信息分别进行授时认证。

[53] 可信授时机构可以是诸如国家授时中心，或者国家授时中心所授权的相应授时机构。可信授时机构接收到上述相关信息的集合，针对任一相关信息，即给出一个可信时间戳，并且对可信时间戳进行数字签名认证，生成一个包含可信时间戳和数字签名的授

时证书，其中授时证书中还可以包含上述目标账本的相关信息。

[54] 其中，相关信息中的账本标识可以写入授时证书的加密信息中，也可以不写入。返回的授时证书中应当携带对应的账本标识，以便在存在多份授时证书时可以区分。数字签名的方式为常规的私钥加密、公钥解密即可。如图 5 所示，图 5 为本说明书实施例所提供的一种授时证书的结构示意图。

[55] S407，接收授时认证机构所返回的授时证书的集合，其中，授时证书包含可信时间戳、所述相关信息和可信授时机构数字签名，授时证书、授时证书中包含的相关信息和目标账本存在一一对应关系。

[56] 服务端可以每次接收到一批授时证书，通过授时证书的账本标识可以明确是对应于哪个账本。

[57] 针对于某一个账本而言，数据库服务段可以接收到一连串的关于该账本的包含时间公正机构签名的可信授时证书，每一个授时证书中包含一个可信时间戳，且对应于一段部分账本。

[58] 一个授时证书可以证明其对应的部分账本是在该可信时间戳之前生成的。通过授时证书中的相关信息可以明确的知道是哪部分账本。数据库服务方可以对一系列的授时证书进行相应的管理，以及验证。例如，数据库服务方可以对每个授时证书进行顺序编号。建立一个关于授时证书的数据库或者索引。在数据库或者索引中包含有起始数据块高、结束数据块高、授时证书对应的部分账本的根哈希值和授时证书编号的对应关系表。如图 6 所示，图 6 为数据库服务端中对于多份账本的授时证书的示意图。

[59] 通过本说明书实施例所提供的方案，在进行授时认证时，可以对需要进行授时认证的目标账本进行批量申请，从而避免每个账本单独申请授时认证，提高效率，便于管理。

[60] 在一种实施例中，进行批量认证之前，为避免一次性认证的目标账本过多，可以预先设置相应的授时认证条件，以对相关信息的集合进行拆分。

[61] 具体而言，可以包括：将包含指定数量的相关信息的集合发送至可信授时机构，例如，指定在一次认证过程中，相关信息的集合中包含的相关信息不超过 100 份。或者，将不超过指定占用空间的相关信息的集合发送至可信授时机构，例如，指定在一次认证过程中，相关信息的集合的占用空间不超过 1M。

[62] 在一种实施例中，服务端可以向用户提供授时认证注册服务，只有通过了授时认证注册的账本才可以进行授时注册。在注册服务中，用户可以注册需要进行注册的账本标识、以及授时认证的时间粒度。例如，用户选择可以每 10 天进行一次授时认证（即，将每 10 天内生成的数据块作为目标账本进行授时认证），或者，选择每 30 天进行一次授时认证。在实际应用中，进行授时认证由于是通过可信授时机构进行，对于用户而言可能会需要额外的开销，可以让用户根据实际需要自定义进行授时认证的事件粒度，提高用户体验。

[63] 用户注册的授时认证信息可以通过注册信息表的形式进行存储，注册信息表中至包含需要注册的账本标识，以及，包括该账本进行授时认证的时间粒度。从而数据库服务端可以从注册信息表中根据账本标识自动的获取需要进行注册的账本。

[64] 在以注册形式提供授时认证的基础上， 数据库服务端首先会根据用户所选择的时间粒度，将时间粒度相同的账本放到一起进行授时认证。例如，假设授时认证服务分别以时间粒度每 1 天、每 10 天、每 30 天进行一次批量授时认证。即，在数据库服务端中可以生成对应的 3 个时间粒度不同的目标账本的集合，对应的，在发送相关信息的集合时也是分别发送。

[65] 进一步地，如果某个账本在两次进行授时认证的窗口期间内进行了注册，则需要根据该账本所选择时间粒度进行首次注册的时间对齐。例如，在 5 天前已经进行了时间粒度为 10 天的批量授时认证，如果此时，一份账本注册了时间粒度为 10 天的授时认证，则，对于该账本那而言，首次授时认证的时间将会被对齐到 5 天后的下一次时间粒度为 10 天的批量授时认证。

[66] 对应的，本说明书实施例还提供一种块链式账本中的授时认证装置，应用于通过块链式账本存储数据的中心化的数据库服务端中，如图 7 所示，图 7 是本说明书实施例提供的一种块链式账本中的授时认证的结构示意图，包括:

[67] 目标账本确定模块 701，确定需要进行授时认证的目标账本的集合，所述集合中包含至少一个目标账本，其中，所述目标账本至少包含一个数据块，或者包含同一账本中多个块高连续的数据块;

[68] 信息集合生成模块 703，针对集合中的每一目标账本，确定该目标账本进行授时认证时所需包含的相关信息，生成包含相关信息的集合，其中，每一份相关信息对应于一份目标账本，所述相关信息包括该目标账本的标识、起始块高、结束块高、该账目标账

本中数据块构成的默克尔树的根哈希；

[69] 发送模块 705，将所述相关信息的集合发送至可信授时机构，以便可信授时机构对所述集合中的每一份相关信息分别进行授时认证；

[70] 授时证书接收模块 707，接收授时认证机构所返回的授时证书的集合，其中，授时证书包含可信时间戳、所述相关信息和可信授时机构数字签名，授时证书、授时证书中包含的相关信息和目标账本存在一一对应关系。

[71] 进一步地，所述装置还包括数据记录接收模块 709，接收待存储的数据记录，确定各数据记录的哈希值；数据块生成模块 711，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：

[72] 当 N=1 时，初始数据块的哈希值和块高基于预设方式给定；

[73] 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。

[74] 进一步地，在所述装置中，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；或者，距离上一次成块时刻的时间间隔达到时间阈值。

[75] 进一步地，所述发送模块 705，将包含指定数量的相关信息的集合发送至可信授时机构；或者，将不超过指定占用空间的相关信息的集合发送至可信授时机构。

[76] 进一步地，所述目标账本确定模块 701，从预先建立的注册信息表中，根据账本标识确定需要进行授时认证的目标账本，所述注册信息表用于存储已经注册需要进行授时认证的账本标识。

[77] 进一步地，所述发送模块 705，根据注册信息表中目标账本所注册的时间粒度，将时间粒度相同的目标账本所对应的相关信息的集合发送至可信授时机构。

[78] 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 所示的块链式账本中的授时认证方法。

[79] 图 8 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。

[80] 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。

[81] 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。

[82] 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。

[83] 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。

[84] 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。

[85] 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。

[86] 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 所示的块链式账本中的授时认证方法。

[87] 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。

[88] 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。

[89] 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。

[90] 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。

[91] 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、一种块链式账本中的授时认证方法，应用于通过块链式账本存储数据的中心化的数据库服务端中，所述方法包括:

确定需要进行授时认证的目标账本的集合，所述集合中包含至少一个目标账本，其中，所述目标账本至少包含一个数据块，或者包含同一账本中多个块高连续的数据块;

针对集合中的每一目标账本，确定该目标账本进行授时认证时所需包含的相关信息，生成包含相关信息的集合，其中，每一份相关信息对应于一份目标账本，所述相关信息包括该目标账本的标识、起始块高、结束块高、该账目标账本中数据块构成的默克尔树的根哈希;

将所述相关信息的集合发送至可信授时机构，以便可信授时机构对所述集合中的每一份相关信息分别进行授时认证;

接收授时认证机构所返回的授时证书的集合，其中，授时证书包含可信时间戳、所述相关信息和可信授时机构数字签名，授时证书、授时证书中包含的相关信息和目标账本存在一一对应关系。

2、如权利要求 1 所述的方法，在中心化的数据库服务提供方，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。

3、如权利要求 2 所述的方法，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；或者，

距离上一次成块时刻的时间间隔达到时间阈值。

4、如权利要求 1 所述的方法，将所述相关信息的集合发送至可信授时机构，包括:

将包含指定数量的相关信息的集合发送至可信授时机构；或者，

将不超过指定占用空间的相关信息的集合发送至可信授时机构。

5、如权利要求 1 所述的方法，确定需要进行授时认证的目标账本的集合，包括:

从预先建立的注册信息表中，根据账本标识确定需要进行授时认证的目标账本，所

述注册信息表用于存储已经注册需要进行授时认证的账本标识。

6、如权利要求 5 所述的方法，将所述相关信息的集合发送至可信授时机构，包括：

根据注册信息表中目标账本所注册的时间粒度，将时间粒度相同的目标账本所对应的相关信息的集合发送至可信授时机构。

7、一种块链式账本中的授时认证装置，应用于通过块链式账本存储数据的中心化的数据库服务端中，所述装置包括：

目标账本确定模块，确定需要进行授时认证的目标账本的集合，所述集合中包含至少一个目标账本，其中，所述目标账本至少包含一个数据块，或者包含同一账本中多个块高连续的数据块；

信息集合生成模块，针对集合中的每一目标账本，确定该目标账本进行授时认证时所需包含的相关信息，生成包含相关信息的集合，其中，每一份相关信息对应于一份目标账本，所述相关信息包括该目标账本的标识、起始块高、结束块高、该账目标账本中数据块构成的默克尔树的根哈希；

发送模块，将所述相关信息的集合发送至可信授时机构，以便可信授时机构对所述集合中的每一份相关信息分别进行授时认证；

授时证书接收模块，接收授时认证机构所返回的授时证书的集合，其中，授时证书包含可信时间戳、所述相关信息和可信授时机构数字签名，授时证书、授时证书中包含的相关信息和目标账本存在一一对应关系。

8、如权利要求 7 所述的装置，还包括数据记录接收模块，接收待存储的数据记录，确定各数据记录的哈希值；数据块生成模块，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。

9、如权利要求 7 所述的装置，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；或者，距离上一次成块时刻的时间间隔达到时间阈值。

10、如权利要求 7 所述的装置，所述发送模块，将包含指定数量的相关信息的集合发送至可信授时机构；或者，将不超过指定占用空间的相关信息的集合发送至可信授时机构。

11、如权利要求 7 所述的装置，所述目标账本确定模块，从预先建立的注册信息表

中，根据账本标识确定需要进行授时认证的目标账本，所述注册信息表用于存储已经注册需要进行授时认证的账本标识。

12、如权利要求 11 所述的装置，所述发送模块，根据注册信息表中目标账本所注册的时间粒度，将时间粒度相同的目标账本所对应的相关信息的集合发送至可信授时机构。

13、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 1 至 6 任一项所述的方法。

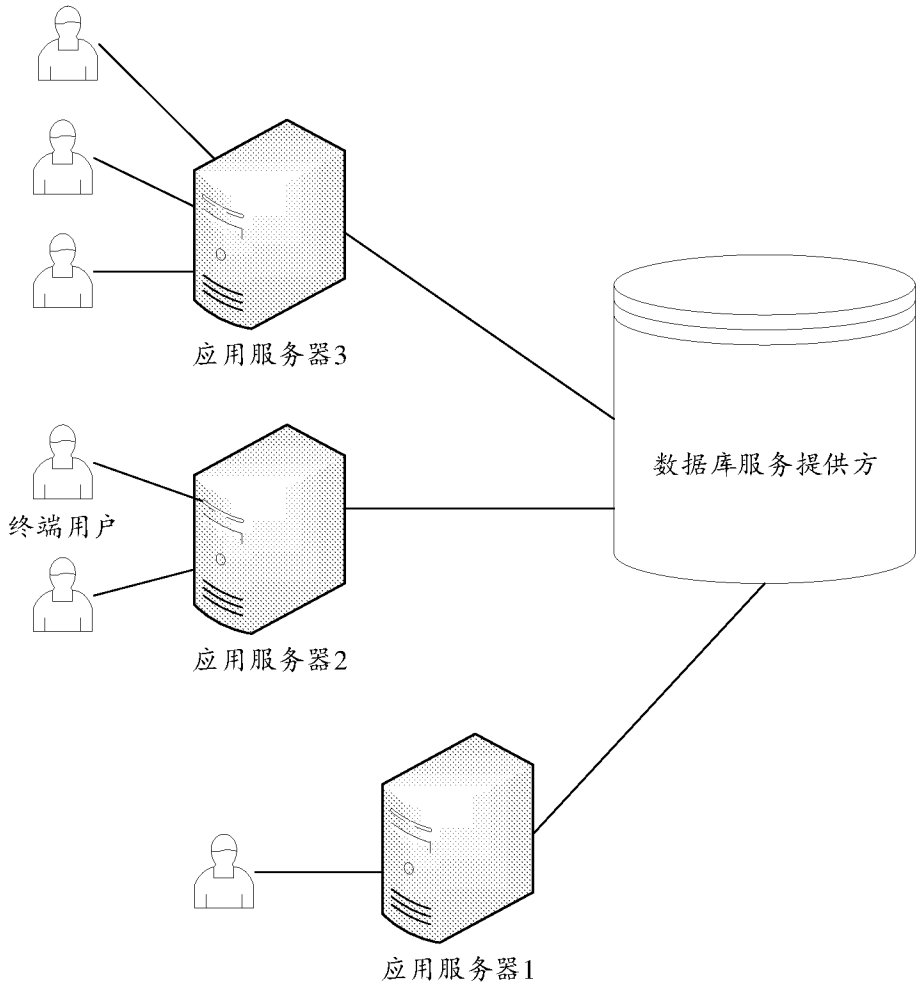

应用服务器3
终端用户
应用服务器2
数据库服务提供方
应用服务器1

图 1

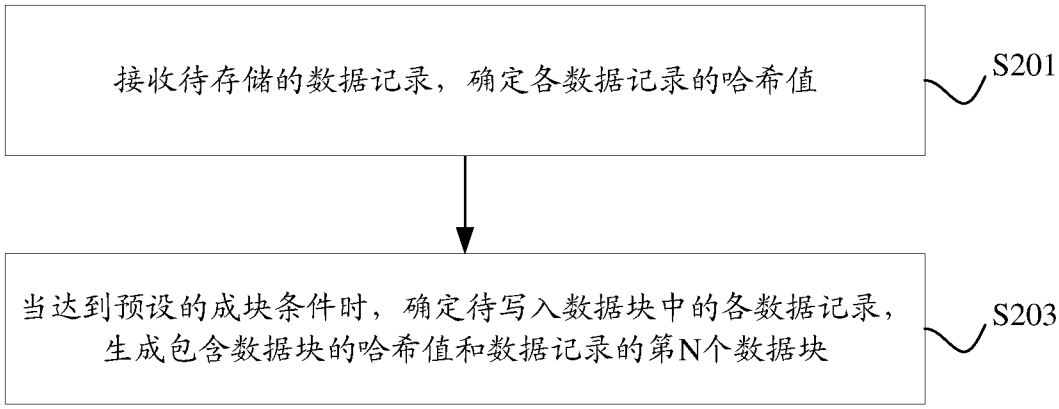

接收待存储的数据记录，确定各数据记录的哈希值
S201
当达到预设的成块条件时，确定待写入数据块中的各数据记录，生成包含数据块的哈希值和数据记录的第N个数据块
S203

图 2

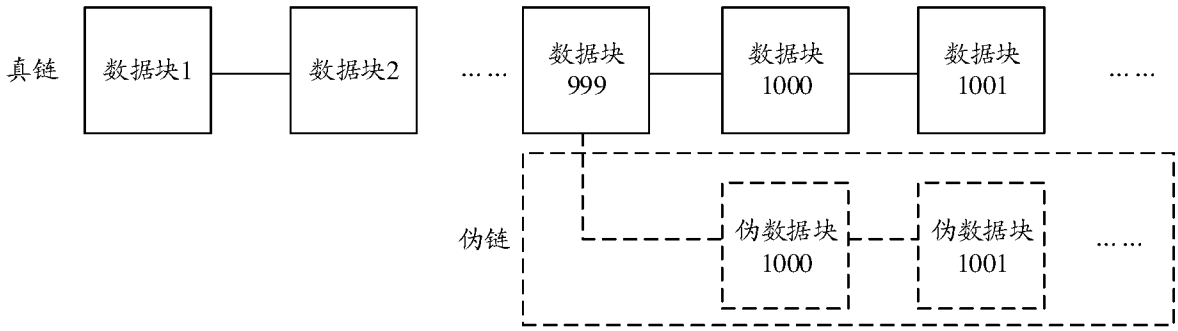

真链
数据块1
数据块2
……
数据块
999
数据块
1000
数据块
1001
……
伪链
伪数据块
1000
伪数据块
1001
……

图 3

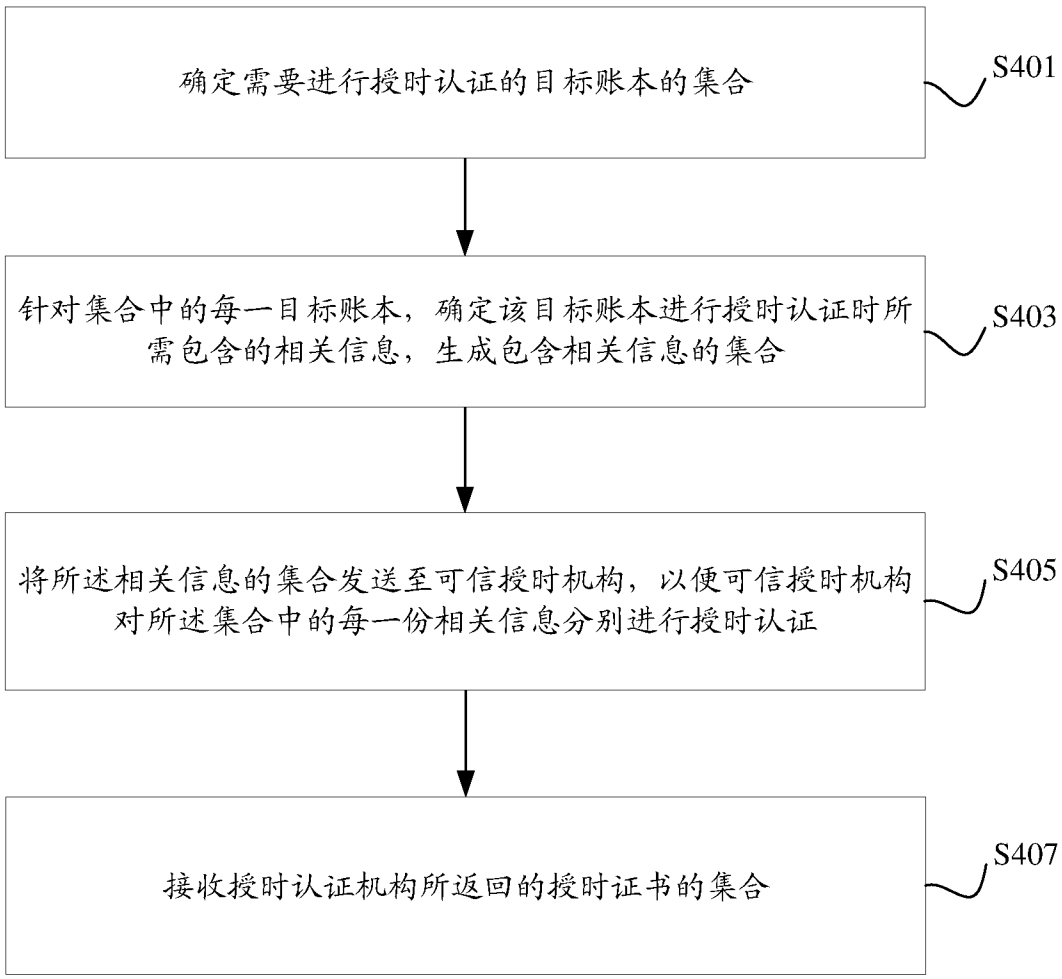

确定需要进行授时认证的目标账本的集合
S401
针对集合中的每一目标账本，确定该目标账本进行授时认证时所需包含的相关信息，生成包含相关信息的集合
S403
将所述相关信息的集合发送至可信授时机构，以便可信授时机构对所述集合中的每一份相关信息分别进行授时认证
S405
接收授时认证机构所返回的授时证书的集合
S407

图 4

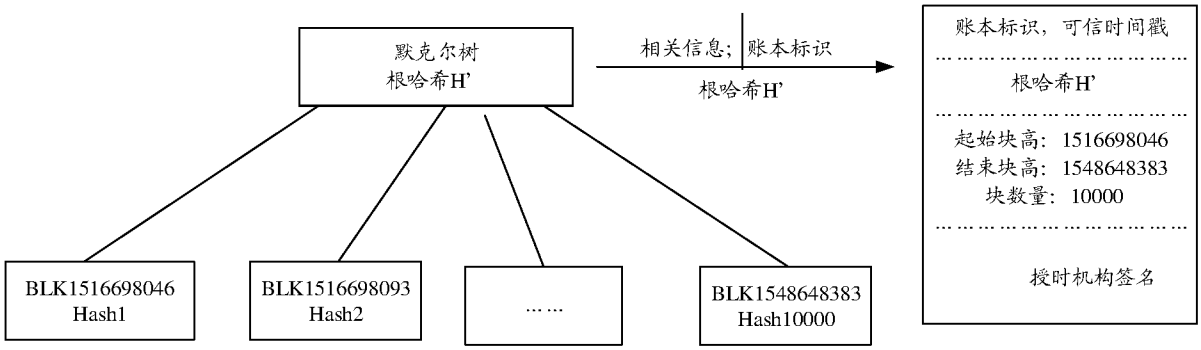

默克尔树
根哈希H'
相关信息；
账本标识
根哈希H'
账本标识，可信时间戳
根哈希H'
起始块高：1516698046
结束块高：1548648383
块数量：10000
授时机构签名
BLK1516698046
Hash1
BLK1516698093
Hash2
……
BLK1548648383
Hash10000

图 5

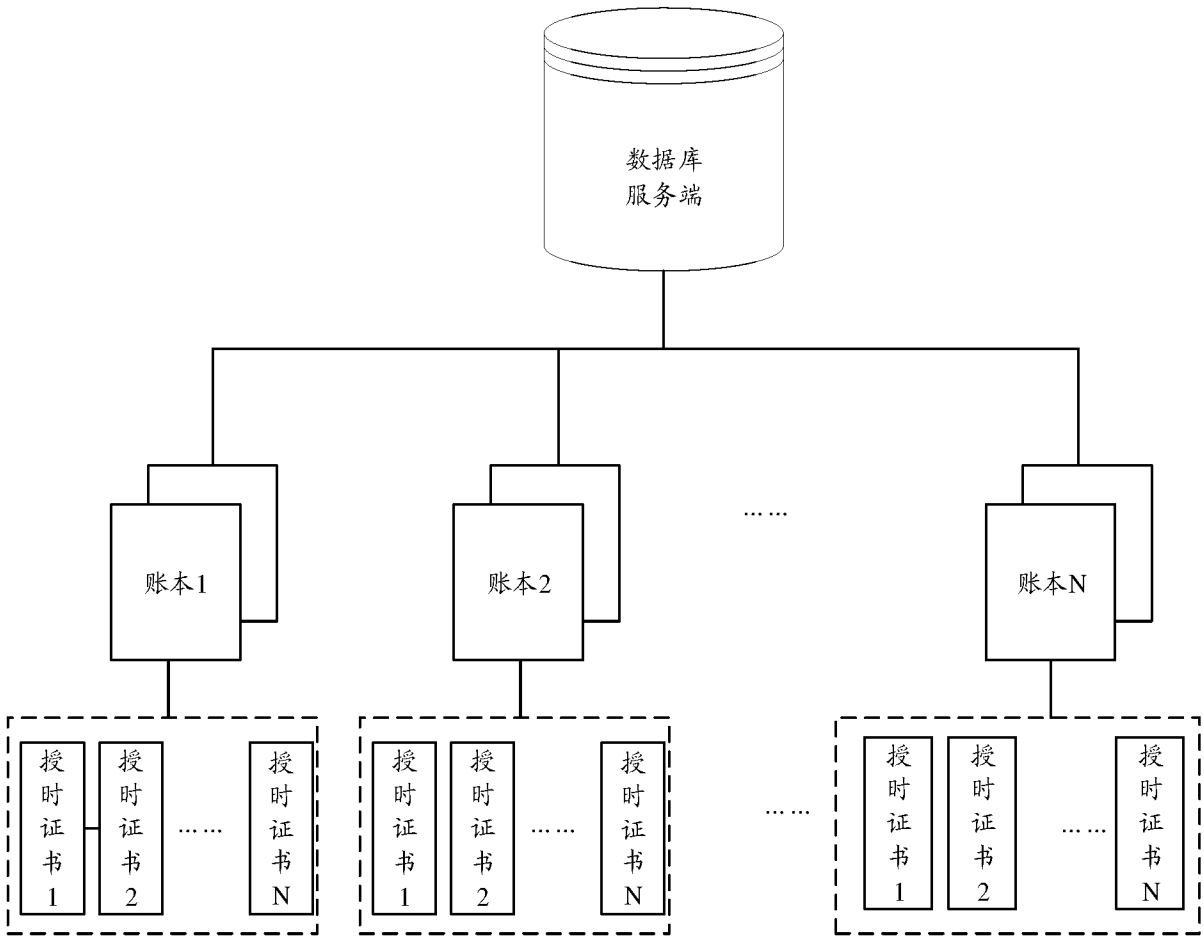

数据库
服务端
账本1
账本2
……
账本N
授时证书1
授时证书2
……
授时证书N

图 6

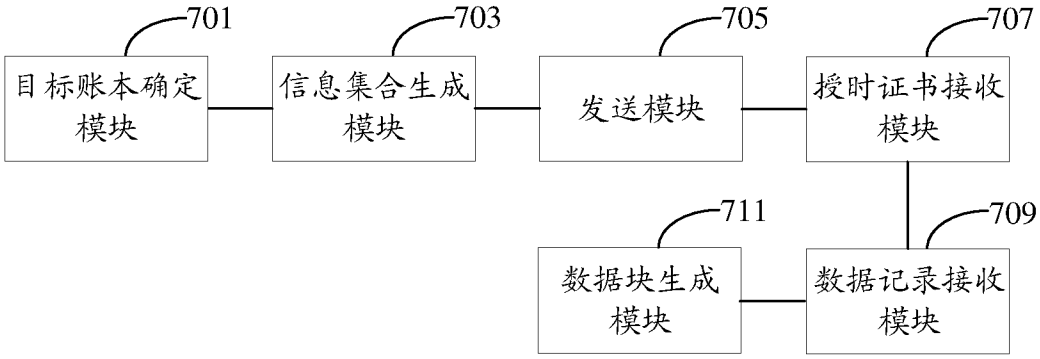

701
目标账本确定模块
703
信息集合生成模块
705
发送模块
707
授时证书接收模块
711
数据块生成模块
709
数据记录接收模块

图 7

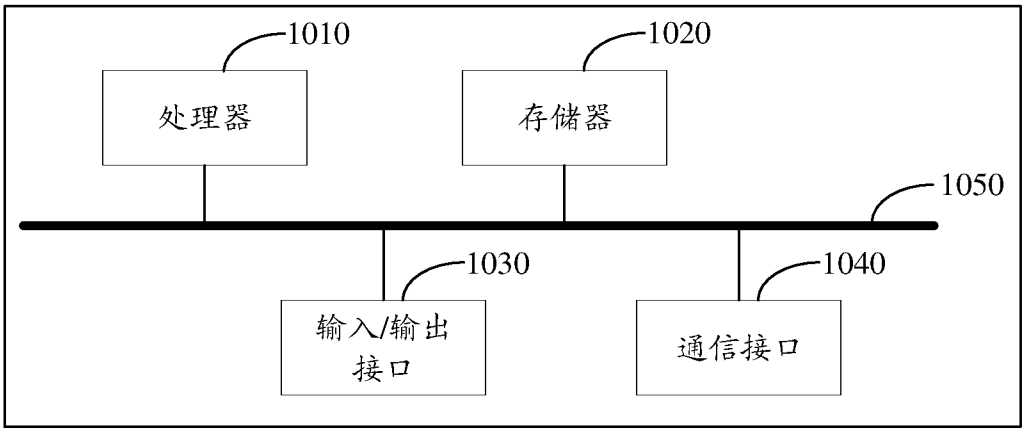

1010
处理器
1020
存储器
1050
1030
输入/输出接口
1040
通信接口

图 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2020/071687

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32(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

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)

CNABS; CNTXT; VEN; CNKI; WOTXT; EPTXT; USTXT; 百度: 区块链, 块链, 以太坊, 比特币, 联盟链, 认证, 授信, 授时, 批量, 集, 集合, 统一, 时间, 时钟, 账本, blockchain, block chain, authentic, authentication, time, clock, group, batch, aggregation, account, Ledger

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110266494 A (ALIBABA GROUP HOLDING LIMITED) 20 September 2019 (2019-09-20) claims 1-13, and description, paragraphs [0004]-[0090]	1-13
X	CN 106407795 A (BEIJING PEERSAFE TECHNOLOGY CO., LTD.) 15 February 2017 (2017-02-15) description, paragraphs [0052]-[0108]	1-13
A	CN 109064324 A (CHONGQING FINANCIAL ASSETS EXCHANGE CO., LTD.) 21 December 2018 (2018-12-21) entire document	1-13
A	EP 3007120 A1 (DPS ENGINEERING GMBH) 13 April 2016 (2016-04-13) entire document	1-13

☐ 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
07 March 2020	**15 April 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/CN2020/071687

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 110266494 A	20 September 2019	None	
CN 106407795 A	15 February 2017	CN 106407795 B	14 May 2019
CN 109064324 A	21 December 2018	None	
EP 3007120 A1	13 April 2016	None	

国际检索报告

国际申请号
PCT/CN2020/071687

A. 主题的分类

H04L 9/32(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

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））

CNABS;CNTXT;VEN;CNKI;WOTXT;EPTXT;USTXT;百度:区块链，块链，以太坊，比特币，联盟链，认证，授信，授时，批量，集，集合，统一，时间，时钟，账本，blockchain，block chain，authentic，authentication，time，clock，group，batch，aggregation，account，Ledger

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 110266494 A (阿里巴巴集团控股有限公司) 2019年 9月 20日 (2019-09-20) 权利要求1-13，说明书[0004]-[0090]段	1-13
X	CN 106407795 A (北京众享比特科技有限公司) 2017年 2月 15日 (2017-02-15) 说明书[0052]-[0108]段	1-13
A	CN 109064324 A (重庆金融资产交易所有限责任公司) 2018年 12月 21日 (2018-12-21) 全文	1-13
A	EP 3007120 A1 (DPS ENGINEERING GMBH) 2016年 4月 13日 (2016-04-13) 全文	1-13

☐ 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 7日	2020年 4月 15日

ISA/CN的名称和邮寄地址	受权官员
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	薛乐梅
传真号 (86-10)62019451	电话号码 86-(20)-28950448

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2020/071687

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 110266494 A	2019年 9月 20日	无	
CN 106407795 A	2017年 2月 15日	CN 106407795 B	2019年 5月 14日
CN 109064324 A	2018年 12月 21日	无	
EP 3007120 A1	2016年 4月 13日	无	