(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
2018 年 10 月 11 日 (11.10.2018)

WIPO | PCT

(10) 国际公布号
WO 2018/184447 A1

(51) 国际专利分类号:
H04L 9/32 (2006.01)

(21) 国际申请号: PCT/CN2018/078888

(22) 国际申请日: 2018 年 3 月 13 日 (13.03.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201710218253.X 2017年4月5日 (05.04.2017) CN

(71) 申请人: 中国移动通信有限公司研究院 (CHINA MOBILE COMMUNICATION LTD., RESEARCH INSTITUTE) [CN/CN]; 中国北京市西城区宣武门西大街32号, Beijing 100053 (CN)。
中国移动通信集团有限公司 (CHINA MOBILE COMMUNICATIONS GROUP CO., LTD.) [CN/CN]; 中国北京市西城区金融大街29号, Beijing 100032 (CN)。

(72) 发明人: 阎军智 (YAN, Junzhi); 中国北京市西城区宣武门西大街32号, Beijing 100053 (CN)。

(74) 代理人: 北京派特恩知识产权代理有限公司 (CHINA PAT INTELLECTUAL PROPERTY OFFICE); 中国北京市海淀区海淀南路21号中关村知识产权大厦B座2层, Beijing 100080 (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:** BLOCKCHAIN-BASED DIGITAL CERTIFICATE DELETION METHOD, DEVICE AND SYSTEM, AND STORAGE MEDIUM

(54) **发明名称**: 基于区块链的数字证书删除方法、装置及系统、存储介质

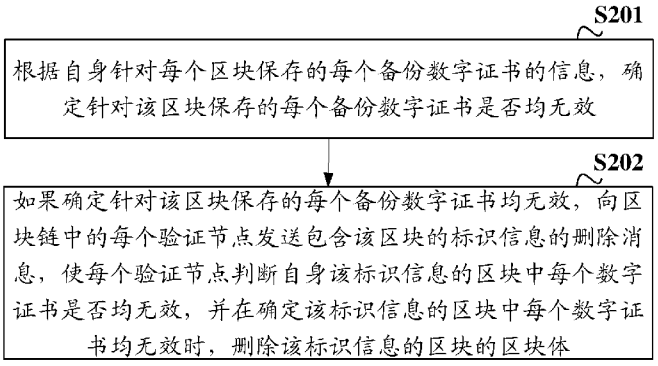

图 2

S201 Determine, according to information of respective backup digital certificates locally stored for each block, whether the respective backup digital certificates stored for the block are invalid

S202 If the respective backup digital certificates stored for the block are determined to be invalid, transmit, to each verification node in a blockchain, a deletion message comprising identifier information of the block, such that the verification node determines whether respective digital certificates in the block associated with the identifier information are invalid, and if so, delete a body of the block associated with the identifier information

(57) **Abstract:** Provided are a blockchain-based digital certificate deletion method, device and system, and a storage medium. The method comprises: if respective backup digital certificates stored for each block are invalid according to information of the respective backup digital certificates stored locally for the block, transmitting, to each verification node, a deletion message comprising identifier information of the block, such that the verification node deletes a body of the block when respective digital certificates in the block associated with the identifier information are determined to be invalid.

(57) **摘要**: 一种基于区块链的数字证书删除方法、装置及系统、存储介质。方法包括: 根据自身针对每个区块保存的每个备份数字证书的信息, 如果针对该区块保存的每个备份数字证书均无效, 向每个验证节点发送包含该区块的标识信息的删除消息, 使每个验证节点确定自身该标识信息的区块中每个数字证书均无效时, 删除该区块的区块体。

[见续页]

WO 2018/184447 A1

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))。

基于区块链的数字证书删除方法、装置及系统、存储介质

相关申请的交叉引用

本申请基于申请号为201710218253.X、申请日为2017年04月05日的中国专利申请提出，并要求该中国专利申请的优先权，该中国专利申请的全部内容在此引入本申请作为参考。

技术领域

本公开实施例涉及网络安全技术领域，尤其涉及一种基于区块链的数字证书删除方法、装置及系统。

背景技术

数字证书是一种由权威机构颁发的用于在网络上证明用户身份的文件，颁发数字证书的过程也可以称为认证授权（Certification Authority，CA）过程。现有公钥基础设施（Public Key Infrastructure，PKI）技术中，CA是信任的起点，如果能够控制一个CA，那么就可以利用该CA机构随意签发数字证书，因此，处于核心的CA极易遭受攻击。一旦某个CA被破坏，那么该CA签发的所有数字证书都不再安全，不能继续使用。除此之外，数字证书依赖方事先安装或预置的CA根数字证书也有可能被攻击，如果根数字证书被恶意篡改，那么将影响整个数字证书验证过程，甚至可能将虚假用户数字证书识别为合法的用户数字证书。

近年来兴起的区块链技术，按照时间顺序将存储数字证书的区块以顺序相连的方式进行链式存储，并根据存储在每个区块中的数字证书生成该区块对应的可信树（Merkle）值，用于对该区块中存储的数字证书进行验证防止该区块中存储的数字证书被篡改。同时区块链中的每个验证节点存储

该区块链中的所有数字证书，并同时对生成及调用数字证书的请求进行验证，不存在中心的 CA 节点，即使某个验证节点发生故障或者遭受攻击，也能保证数字证书的正确性。

然而，区块链中却有一个很大的问题，区块链中会包含所有的历史数字证书，随着时间的推移，区块链中存储的数字证书会不断的增多，整个区块链存储的数据量会越来越大，需要验证节点的存储和计算资源也越来越多，给验证节点带来严重的负担，影响验证节点的运行和用户的体验。

发明内容

本公开实施例提供一种基于区块链的数字证书删除方法、装置及系统，用以解决现有技术中存在数字证书存储过程中数据量越来越大，需要验证节点的存储和计算资源越来越高，影响验证节点的运行和用户的体验的问题。

本公开实施例公开了一种区块链的数字证书删除方法，所述区块链中包含多个验证节点和至少一个备份节点，所述删除方法应用于区块链中的任一备份节点，所述方法包括:

根据自身针对每个区块保存的每个备份数字证书的信息，确定针对该区块保存的每个备份数字证书是否均无效;

如果确定针对该区块保存的每个备份数字证书均无效，向区块链中的每个验证节点发送包含该区块的标识信息的删除消息，其中，所述删除消息，用于使每个验证节点判断自身该标识信息的区块中每个数字证书是否均无效，并在确定该标识信息的区块中每个数字证书均无效时，删除该标识信息的区块的区块体。

本公开实施例公开了一种基于区块链的数字证书删除方法，所述区块链中包含多个验证节点和至少一个备份节点，所述删除方法应用于区块链中的任一验证节点，所述方法包括:

接收区块链中备份节点发送的包含区块的标识信息的删除消息，其中所述删除消息为区块链中的备份节点根据其自身针对每个区块保存的每个备份数字证书的信息，确定针对该区块保存的每个备份数字证书均无效后发送的；

判断自身保存的该标识信息的区块中每个数字证书是否均无效；

如果确定该标识信息的区块中每个数字证书均无效，删除该区块的区块体。

本公开实施例公开了一种基于区块链的数字证书删除装置，所述区块链中包含多个验证节点和至少一个备份节点，所述删除装置应用于区块链中的任一备份节点，所述装置包括：

确定模块，配置为根据自身针对每个区块保存的每个备份数字证书的信息，确定针对该区块保存的每个备份数字证书是否均无效；

发送模块，配置为如果确定针对该区块保存的每个备份数字证书均无效，向区块链中的每个验证节点发送包含该区块的标识信息的删除消息，使每个验证节点判断自身该标识信息的区块中每个数字证书是否均无效，并在确定该标识信息的区块中每个数字证书均无效时，删除该标识信息的区块的区块体。

本公开实施例公开了一种基于区块链的数字证书删除装置，所述区块链中包含多个验证节点和至少一个备份节点，所述删除装置应用于区块链中的任一验证节点，所述装置包括：

接收模块，配置为接收区块链中备份节点发送的包含区块的标识信息的删除消息，其中所述删除消息为区块链中的备份节点根据其自身针对每个区块保存的每个备份数字证书的信息，确定针对该区块保存的每个备份数字证书均无效后发送的；

判断模块，配置为判断自身保存的该标识信息的区块中每个数字证书

是否均无效；

删除模块，配置为如果确定该标识信息的区块中每个数字证书均无效，删除该区块的区块体。

本公开实施例公开了一种基于区块链的数字证书删除系统，所述删除系统包括至少一个上述应用于备份节点的基于区块链的数字证书删除装置，及多个上述应用于验证节点的基于区块链的数字证书删除装置。

本公开实施例还公开了一种计算机存储介质，所述计算机存储介质存储有计算可执行指令；所述计算机可执行指令被执行后，能够实现应用于备份节点的基于区块链的数字证书删除方法中的一个或多个，或实现应用于验证节点的基于区块链的数字证书删除方法中的一个或多个。

本公开实施例公开了一种基于区块链的数字证书删除方法、装置及系统，所述区块链中包含多个验证节点和至少一个备份节点，所述删除方法应用于区块链中的任一备份节点，所述方法包括：根据自身针对每个区块保存的每个备份数字证书的信息，确定针对该区块保存的每个备份数字证书是否均无效；如果确定针对该区块保存的每个备份数字证书均无效，向区块链中的每个验证节点发送包含该区块的标识信息的删除消息，使每个验证节点判断自身该标识信息的区块中每个数字证书是否均无效，并在确定该标识信息的区块中每个数字证书均无效时，删除该标识信息的区块的区块体。由于在本公开实施例中，如果备份节点判断针对某一区块保存的每个备份数字证书均无效，向区块链中的每个验证节点发送包含该区块的标识信息的删除消息，使每个验证节点判断自身该标识信息的区块中每个数字证书是否均无效，并在确定该标识信息的区块中每个数字证书均无效时，删除该标识信息的区块的区块体，减少了数据证书存储过程中占用的存储空间，节约了验证节点的存储和在后续进行验证时所需计算量，并进一步减少了所消耗的计算资源，提高了验证节点的运行效率（例如，验证

效率）和用户的体验。

附图说明

图 1 为本公开提供的一种区块链架构示意图；

图 2 为本公开实施例 1 提供的一种基于区块链的数字证书删除过程示意图；

图 3 为本公开实施例 1 和实施例 4 提供的一种验证节点存储数字证书的存储结构示意图；

图 4 为本公开实施例 4 提供的一种基于区块链的数字证书删除过程示意图；

图 5 为本公开实施例 7 提供的一种基于区块链的数字证书删除装置结构示意图；

图 6 为本公开实施例 8 提供的一种基于区块链的数字证书删除装置结构示意图；

图 7 为本公开实施例 9 提供的一种基于区块链的数字证书删除系统结构示意图。

具体实施方式

下面将结合本公开实施例中的附图，对本公开实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本公开实施例一部分实施例，而不是全部的实施例。基于本公开实施例中的实施例，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，都属于本公开实施例保护的范围。

图 1 为本公开实施例提供的一种区块链架构示意图，在该区块链中包含多个验证节点和至少一个备份节点，每个验证节点用于验证用户对数字

证书的生成请求及用户对数字证书状态的更新请求。每个验证节点按照预设的时间顺序依次产生新的区块，并根据数字证书生成时间将数字证书存储到对应的区块中，还用于根据用户对数字证书状态的更新请求对存储的数字证书的状态进行更新。备份节点用于针对验证节点的每个区块，备份存入该区块的每个数字证书，并根据用户对数字证书状态的更新请求对针对每个区块备份的数字证书的状态进行更新。

实施例 1:

图 2 为本公开实施例提供的一种基于区块链的数字证书删除过程示意图，该过程包括:

S201: 根据自身针对每个区块保存的每个备份数字证书的信息，确定针对该区块保存的每个备份数字证书是否均无效。

本公开实施例实施例提供的一种基于区块链的数字证书删除方法，应用于区块链中的任一备份节点，该备份节点可以是具有运算和存储功能的个人电脑（Personal Computer，PC）机、服务器等设备。

在本公开实施例实施例中，因为在区块链中如果未遭到恶意更改，每个验证节点的每个对应区块中保存的数字证书是相同的，而备份节点对区块链中每个验证节点的每个区块保存的数字证书进行备份，即针对验证节点保存的每个区块中的数字证书进行备份，在备份节点中针对每个区块保存有该区块中每个数字证书对应的备份数字证书。

可选地，备份节点根据自身针对每个区块保存的每个备份数字证书的信息，确定针对该区块保存的每个备份数字证书是否均无效，其中备份数字证书的信息可以是该数字证书的有效期。一个区块内保存有多个备份数字证书，若该区域内每一个备份数字证书均失效了，则表明该区块的区块体内的每个数字证书均无效，则至少可以删除该区块的区块体了，故生成所述删除消息。

例如：备份节点针对区块 A 保存有备份数字证书 1、备份数字证书 2，针对区块 B 保存有备份数字证书 3、备份数字证书 4。当前时间 2017 年 3 月 29 日，针对区块 A 备份节点根据备份数字证书 1 的有效期 2015 年 7 月 1 日-2016 年 7 月 1 日，确定备份数字证书 1 的有效期过期，备份数字证书 1 无效，根据备份数字证书 2 的有效期 2016 年 2 月 1 日-2017 年 2 月 1 日，确定备份数字证书 2 的有效期过期，备份数字证书 2 无效，针对区块 A 保存的备份数字证书 1、备份数字证书 2 均无效，确定针对区块 A 保存的每个备份数字证书均无效；针对区块 B 备份节点根据备份数字证书 3 的有效期 2015 年 7 月 5 日-2016 年 7 月 5 日，确定备份数字证书 3 的有效期过期，备份数字证书 3 无效，根据备份数字证书 4 的有效期 2016 年 5 月 1 日-2017 年 5 月 1 日，确定备份数字证书 4 的有效期未过期，备份数字证书 4 有效，针对区块 B 保存的备份数字证书 4 有效，确定针对区块 B 保存的每个备份数字证书中存在有效的备份数字证书。

S202：如果确定针对该区块保存的每个备份数字证书均无效，向区块链中的每个验证节点发送包含该区块的标识信息的删除消息。该删除消息可以使每个验证节点判断自身该标识信息的区块中每个数字证书是否均无效，并在确定该标识信息的区块中每个数字证书均无效时，删除该标识信息的区块的区块体。

区块链中的每个区块由区块头和区块体组成，区块头中保存有该区块产生的时间，父区块哈希值，即该区块产生的时间之前的上一区块的哈希值，根据该区块中保存的每个数字证书确定的 Merkle 值，区块体中保存有记录在该区块的每个数字证书。图 3 为本公开实施例实施例提供的一种验证节点存储数字证书的存储结构示意图，验证节点按照时间顺序依次存储有创世区块、区块 2…区块 n，其中每个区块由区块头和区块体组成，每个区块体中保存有存储在该区块的每个数字证书。

可选地，如果备份节点确定针对该区块保存的每个备份数字证书均无效，则说明针对该区块保存的每个备份数字证书均可删除，向区块链中的每个验证节点发送包含该区块的标识信息的删除消息，如果验证节点每个区块中保存的数字证书与备份节点保存的备份数字证书相同，验证节点可以直接删除自身所述标识信息的区块的区块体，但是为了保证对数字证书删除的准确性，避免错误删除有效的数字证书，在用户需要对数字证书进行验证时，无法通过该错误删除的有效的数字证书，对用户的权益造成损害，在本公开实施例实施例中验证节点接收到包含该区块的标识信息的删除消息后，判断自身该标识信息的区块中每个数字证书是否均无效，并在确定该标识信息的区块中每个数字证书均无效时，删除该标识信息的区块的区块体。

例如：备份节点针对区块 A 保存的每个备份数字证书均无效，则说明针对该区块 A 保存的每个备份数字证书均可删除，向区块链中的每个验证节点发送包含区块 A 标识信息 00001 的删除消息，验证节点接收到包含标识信息 00001 的删除消息后，通过标识信息 00001 识别自身保存的该标识信息的区块 A，验证自身区块 A 中每个数字证书是否均无效，如果自身区块 A 中每个数字证书均无效，删除该区块 A 的区块体。

由于在本公开实施例中，如果备份节点判断针对某一区块保存的每个备份数字证书均无效，向区块链中的每个验证节点发送包含该区块的标识信息的删除消息，使每个验证节点判断自身该标识信息的区块中每个数字证书是否均无效，并在确定该标识信息的区块中每个数字证书均无效时，删除该标识信息的区块的区块体，减少了数据证书存储过程中占用的存储空间，节约了验证节点的存储和计算资源，提高了验证节点的运行效率和用户的体验。

实施例 2:

为了更准确的确定针对每个区块保存的每个备份数字证书是否均无效，在上述实施例的基础上，在本公开实施例中，所述根据自身针对每个区块保存的每个备份数字证书的信息，确定针对该区块保存的每个备份数字证书是否均无效包括:

根据自身针对每个区块保存的每个备份数字证书的信息，确定针对该区块保存的每个备份数字证书的有效期是否过期和/或备份数字证书是否已吊销状态；如备份数字证书的有效期已经超过了，则表示该证书已过期，相当于该备份数字证书已无效。若一个备份数字证书的状态为吊销状态，即该备份数字证书已吊销，从而该备份数据证书已失效。

如果针对该区块保存的每个备份数字证书为有效期过期和/或备份数字证书已吊销，确定针对该区块保存的每个备份数字证书均无效。

在本公开实施例实施例中，备份数字证书的信息包括：备份数字证书的有效期及备份数字证书的状态信息，其中备份数据证书的状态信息包括:签发、吊销、挂起、恢复等，备份节点可以通过识别备份数字证书的状态信息，确定备份数字证书是否已吊销状态，可选地，对备份数字证书状态信息的识别是现有技术不再进行赘述。备份节点可以根据自身针对每个区块保存的每个备份数字证书的有效期是否均过期，确定针对该区块保存的每个备份数字证书是否均无效；当然了，也可以根据自身针对每个区块保存的每个备份数字证书的状态是否均为吊销，确定针对该区块保存的每个备份数字证书是否均无效。

可选地，可以同时根据自身针对每个区块保存的每个备份数字证书的有效期是否过期和该备份数字证书是否已吊销，确定针对每个区块保存的每个备份数字证书是否均无效。如果针对该区块保存的每个备份数字证书均满足该备份数字证书的有效期过期和/或该备份数字证书已吊销，确定针对该区块保存的每个备份数字证书均无效。在本公开实施例实施例中，针

对每个备份数字证书，如果该备份数字证书的有效期为过期，或者该备份数字证书已吊销，则确定该备份数字证书无效。

例如：备份节点针对区块 C 保存有备份数字证书 5、备份数字证书 6，其中备份数字证书 5 的有效期为 2015 年 7 月 5 日-2016 年 7 月 5 日，状态为未吊销，备份数字证书 6 的有效期为 2016 年 7 月 5 日-2017 年 7 月 5 日，状态为吊销，当前时间为 2017 年 3 月 29 日，备份数字证书 5 的有效期过期，备份数字证书 6 的状态为吊销，确定针对区块 C 保存的每个备份数字证书均无效。

实施例 3:

为了防止因备份节点的证书被恶意篡改造成验证节点对自身保存的数字证书的错误删除，在上述各实施例的基础上，在本公开实施例中，如果所述区块链中的每个验证节点的每个区块中保存的每个数字证书使用预设的算法进行变换，所述向区块链中的每个验证节点发送包含该区块的标识信息的删除消息后，所述方法还包括:

将自身针对所述标识信息的区块保存的每个备份数字证书发送给每个验证节点。

为了保证区块链中每个验证节点保存的数字证书数据安全性，区块链中的每个验证节点可以根据预先的设定，对每个区块中保存的每个数字证书使用预设的算法进行变换。例如：验证节点对每个区块保存的每个数字证书使用散列算法进行散列运算，每个区块保存进行散列运算后的每个数字证书。在本公开实施例中，如果验证节点对每个区块保存的每个数字证书使用预设的算法进行变换，备份节点针对区块链中的每个区块备份该区块中保存的使用预设的算法进行变换之前的每个数字证书。

可选地，如果区块链中的每个验证节点的每个区块中保存的每个数字证书使用预设的算法进行变化，备份节点根据自身针对每个区块保存的每

个备份数字证书的信息，确定针对该区块保存的每个备份数字证书均无效后，向区块链中的每个验证节点发送包含该区块的标识信息的删除消息后，还将自身针对所述标识信息的区块保存的每个备份数字证书发送给每个验证节点，验证节点收到备份节点发送的包含该区块的标识信息的删除消息和针对所述标识信息的区块保存的每个备份数字证书后，根据所述标识信息确定自身该标识信息的区块，并采用预设的算法将备份节点针对该标识信息的区块保存的每个备份数字证书进行变换，通过判断自身该标识信息的区块保存的每个数字证书是否均与该备份数字证书变换后的数字证书对应匹配，从而确定备份节点针对该标识信息的区块保存的每个备份数字证书是否正确。

例如：区块链中的每个验证节点的每个区块中保存的每个数字证书使用散列算法进行变化，备份节点确定针对标识信息为 00005 的区块 E 保存的每个备份数字证书均无效，备份节点向区块链中每个验证节点发送包括标识信息 00005 的删除消息后，并将自身针对标识信息为 00005 的区块 E 保存的每个备份数字证书发送给区块链中的每个验证节点。

验证节点接收到包含标识信息 00005 的删除消息和针对标识信息 00005 的区块保存的每个备份数字证书后，根据标识信息 00005 识别自身标识信息为 00005 的区块 E，采用预设的散列算法将备份节点针对标识信息 00005 的区块保存的每个备份数字证书进行散列运算，判断自身区块 E 中保存的每个数字证书是否均与散列运算后的备份数字证书对应匹配，如果是，确定备份节点针对区块 E 保存的每个备份数字证书正确。

实施例 4:

图 4 为本公开实施例提供的一种基于区块链的数字证书删除过程示意图，该过程包括:

S401: 接收区块链中备份节点发送的包含区块的标识信息的删除消息，

其中所述删除消息为区块链中的备份节点根据其自身针对每个区块保存的每个备份数字证书的信息，确定针对该区块保存的每个备份数字证书均无效后发送的。

本公开实施例实施例提供的一种基于区块链的数字证书删除方法，应用于区块链中的任一验证节点，该验证节点可以是具有运算和存储功能的PC机、服务器等设备。

在本公开实施例中，因为在区块链中如果未遭到恶意更改，每个验证节点的每个对应区块中保存的数字证书是相同的，而备份节点对区块链中每个验证节点的每个区块保存的数字证书进行备份，即针对验证节点保存的每个区块中的数字证书进行备份，在备份节点中针对每个区块保存有该区块中每个数字证书对应的备份数字证书。备份节点根据自身针对每个区块保存的每个备份数字证书的信息，确定针对该区块保存的每个备份数字证书是否均无效，如果针对该区块中保存的每个备份数字证书均无效，向区块链中每个验证节点发送包含该区块的标识信息的删除消息。

例如：备份节点针对区块A保存有备份数字证书1、备份数字证书2，当前时间2017年3月29日，针对区块A备份节点根据备份数字证书1的有效期2015年7月1日-2016年7月1日，确定备份数字证书1的有效期过期，备份数字证书1无效，根据备份数字证书2的有效期2016年2月1日-2017年2月1日，确定备份数字证书2的有效期过期，备份数字证书2无效，针对区块A保存的备份数字证书1、备份数字证书2均无效，确定针对区块A保存的每个备份数字证书均无效，向区块链中的每个验证节点发送包含该区块A的标识信息00001的删除消息。

可选地，验证节点接收区块链中备份节点根据其自身针对每个区块保存的每个备份数字证书的信息，确定针对该区块保存的每个备份数字证书均无效后，发送的包含该区块的标识信息的删除消息。

S402: 判断自身保存的该标识信息的区块中每个数字证书是否均无效。

可选地，验证节点接收到备份节点发送的包含区块的标识信息的删除消息后，判断自身保存的该标识信息的区块中每个数字证书是否均无效，其中验证节点可以根据数字证书的有效期判断该数字证书是否有效。

例如：验证节点接收到备份节点发送的包含区块的标识信息 00001 的删除消息，识别自身标识信息为 00001 的区块 A，区块 A 保存有数字证书 1、数字证书 2，当前时间 2017 年 3 月 29 日，验证节点根据数字证书 1 的有效期 2015 年 7 月 1 日-2016 年 7 月 1 日，确定数字证书 1 的有效期过期，数字证书 1 无效，根据数字证书 2 的有效期 2016 年 2 月 1 日-2017 年 2 月 1 日，确定数字证书 2 的有效期过期，数字证书 2 无效，针对区块 A 保存的数字证书 1、数字证书 2 均无效，确定标识信息为 00001 的区块 A 中每个数字证书均无效。

S403: 如果确定该标识信息的区块中每个数字证书均无效，删除该区块的区块体。

区块链中的每个区块由区块头和区块体组成，区块头中保存有该区块产生的时间，父区块哈希值，即该区块产生的时间之前的上一区块的哈希值，根据该区块中保存的每个数字证书确定的 Merkle 值，区块体中保存有记录在该区块的每个数字证书。图 3 为本公开实施例实施例提供的一种验证节点存储数字证书的存储结构示意图，验证节点按照时间顺序依次存储有创世区块、区块 2...区块 n，其中每个区块由区块头和区块体组成，每个区块体中保存有存储在该区块的每个数字证书。

可选地，如果验证节点确定该标识信息的区块中每个数字证书均无效，则说明该区块中每个数字证书均可删除，删除该区块用于存储数字证书的区块体；如果验证节点确定该标识信息的区块中存在至少一个有效的数字证书，则说明该区块中存在不可删除的数字证书，丢弃所述备份节点发送

的所述删除消息，不对该区块做任何处理。

例如：验证节点确定标识信息为 00001 的区块 A 中每个数字证书均无效，则删除区块 A 用于存储数字证书的区块体。

由于在本公开实施例中，验证节点根据备份节点根据其自身针对每个区块保存的每个备份数字证书的信息，判断针对某一区块保存的每个备份数字证书均无效后发送的包含该区块的标识信息的删除消息，确定自身该标识信息的区块中每个数字证书均无效后，删除该标识信息的区块的区块体，减少了数据证书存储过程中占用的存储空间，节约了的存储和计算资源，提高了的运行效率和用户的体验。

实施例 5:

为了防止因备份节点的证书被恶意篡改造成对自身保存的数字证书的错误删除，在上述各实施例的基础上，在本公开实施例中，如果对每个区块保存的每个数字证书使用预设的算法进行变换，所述接收区块链中备份节点发送的包含区块的标识信息的删除消息后，所述方法还包括:

接收所述备份节点发送的所述备份节点针对所述标识信息的区块保存的每个备份数字证书;

所述判断自身保存的该标识信息的区块中每个数字证书的是否均无效之前，所述方法还包括:

采用所述预设的算法对所述每个备份数字证书进行变换;

针对所述标识信息的区块中保存的每个数字证书，判断自身保存的每个数字证书是否均与该备份数字证书变换后的数字证书对应匹配;

如果是，进行后续步骤。该后续步骤至少包括：判断自身保存的该标识信息的区块中每个数字证书的是否均无效的步骤。

为了保证区块链中每个验证节点保存的数字证书数据安全性，验证节点可以根据预先的设定，使用预设的算法对每个区块保存的每个数字证书

使用预设的算法进行变换，例如：验证节点对每个区块中保存的每个数字证书使用散列算法进行散列运算，针对每个区块保存进行散列运算后的每个数字证书。在本公开实施例中，如果验证节点对每个区块保存的每个数字证书使用预设的算法进行变换，备份节点针对区块链中的每个区块备份该区块中保存的使用预设的算法进行变换之前的每个数字证书，并且保存有每个数字证书的信息。

可选地，如果验证节点对每个区块中保存的每个数字证书使用预设的算法进行变化，验证节点接收区块链中备份节点发送的包含区块标识的删除消息后，接收所述备份节点发送的所述备份节点针对所述标识信息的区块保存的每个备份数字证书。

另外，为了防止备份节点针对该标识信息的区块保存的备份数字证书被恶意篡改，验证节点在判断自身保存的该标识的区块中每个数字证书是否均无效之前，还需判断备份节点发送的所述每个备份数字证书是否正确，可选地，验证节点使用预设的算法对所述每个备份数字证书进行变换，通过判断自身针对该标识信息的区块中保存的每个数字证书，即采用预设的算法进行变换后的数字证书，是否均与该备份数字证书变换后的数字证书对应匹配，如果对应匹配，则确定所述备份节点针对该标识信息的区块保存的每个备份数字证书未被篡改，备份节点针对该标识信息的区块保存的每个备份数字证书正确。此时因为备份节点已经判断该标识信息的区块中保存的每个备份数字证书均无效，则验证节点也可以将该标识信息的区块的区块体删除，但因为备份节点保存的备份证书的可靠性不是很高，为了进一步保证数字证书的安全性，该验证节点验证自身该标识信息的区块中每个数字证书是否无效。

如果验证节点使用预设的算法对所述每个备份数字证书进行变换，判断自身针对该标识信息的区块中保存的每个数字证书，即采用预设的算法

进行变换后的数字证书，不能均与该备份数字证书变换后的数字证书对应匹配，则说明所述备份节点针对该标识信息的区块保存的每个备份数字证书中存在至少一个备份数字证书被篡改，为了保证自身保存的数字证书的正确性，避免错误的删除有效的不可删除的数字证书，验证节点丢弃所述备份节点发送的所述删除消息，不对该标识信息的区块做任何处理。

实施例 6:

为了准确的确定自身区块中每个数字证书是否均无效，在上述各实施例的基础上，在本公开实施例中，所述判断自身保存的该标识信息的区块中每个数字证书是否均无效包括:

获取自身保存的该标识信息的区块中每个数字证书的有效期及状态信息;

判断该标识信息的区块中每个数字证书的有效期是否过期和/或数字证书是否已吊销;

如果该标识信息的区块中每个数字证书为有效期过期和/或数字证书的状态为吊销，确定该标识信息的区块中每个数字证书均无效。

在本公开实施例实施例中，数字证书的信息包括：数字证书的有效期及数字证书的状态信息，其中数据证书的状态信息包括：签发、吊销、挂起、恢复等，验证节点可以通过识别数字证书的状态信息，确定数字证书是否已吊销，可选地，对数字证书状态信息的识别是现有技术不再进行赘述。如果没有针对验证节点预先设定，验证节点对每个区块中保存的每个数字证书使用预设的算法进行变换，验证节点根据自身保存的该标识信息的区块中每个数字证书的信息，识别该标识信息的区块中保存的每个未经变换的每个数字证书的有效期，验证节点可以根据自身保存的该标识信息的区块中每个数字证书的有效期是否均过期，确定该标识信息的区块中每个数字证书是否均无效；当然了，也可以根据自身保存的该标识信息的区

块中每个数字证书的状态是否均为吊销，确定该标识信息的区块中每个数字证书是否均无效。

可选地，可以同时根据自身保存的该标识信息的区块中每个数字证书的有效期是否过期和该数字证书是否已吊销，确定该标识信息的区块中每个数字证书是否均无效。如果针对该标识信息的区块中每个数字证书均满足该数字证书的有效期过期和/或该数字证书的状态为吊销，确定该标识信息的区块中每个数字证书均无效。在本公开实施例实施例中，针对每个数字证书，如果该数字证书的有效期为过期，或者该数字证书的状态为吊销，则确定该数字证书无效。

例如：备份节点发送的删除消息包含的区块的标识信息为 00003，验证节点自身标识信息为 00003 的区块 C 中保存有数字证书 5、数字证书 6，其中数字证书 5 的有效期为 2015 年 7 月 5 日-2016 年 7 月 5 日，状态为未吊销，数字证书 6 的有效期为 2016 年 7 月 5 日-2017 年 7 月 5 日，状态为吊销，当前时间为 2017 年 3 月 29 日，数字证书 5 的有效期过期，数字证书 6 的证书状态为吊销，确定自身标识信息为 00003 的区块 C 中每个数字证书均无效。

另外，如果为了保证区块链中每个验证节点保存的数字证书数据安全性，针对验证节点预先设定，验证节点对每个区块中保存的每个数字证书使用预设的算法进行变换，因数字证书的有效期记录在数字证书中，验证节点不能识别该标识信息的区块保存的每个变换后的数字证书的有效期，为了使验证节点判断自身保存的该标识信息的区块中每个数字证书是否均无效，在本公开实施例实施例中，如果验证节点针对备份节点发送的每个备份数字证书，判断自身针对所述标识信息的区块中保存的每个数字证书均与该备份数字证书变换后的数字证书对应匹配，验证节点根据接收到的备份节点发送的所述备份节点针对所述标识信息的区块保存的每个备份数

字证书及自身保存的每个数字证书的状态信息，判断自身保存的该标识信息的区块中每个数字证书是否均无效。

可选地，验证节点根据该标识信息的区块中每个数字证书是否已吊销和/或接收到的每个备份数字证书的有效期是否过期，确定该标识信息的区块中每个数字证书是否均无效。如果该标识信息的区块中每个数字证书均满足该数字证书的状态为吊销和/或接收到的每个备份数字证书为有效期过期，确定该标识信息的区块中每个数字证书均无效。在本公开实施例实施例中，针对每个数字证书，如果该数字证书的状态信息为吊销，或与该数字证书对应匹配的备份数字证书为有效期过期，则确定该数字证书无效。

例如：区块链中的每个验证节点的每个区块中保存的每个数字证书使用散列算法进行变化，备份节点确定针对标识信息为 00005 的区块 E 保存的每个备份数字证书均无效，备份节点向区块链中每个验证节点发送包括标识信息 00005 的删除消息后，并将自身针对标识信息为 00005 的区块 E 保存的每个备份数字证书发送给区块链中的每个验证节点。

验证节点接收到包含标识信息 00005 的删除消息和针对标识信息 00005 的区块保存的每个备份数字证书后，根据标识信息 00005 识别自身标识信息为 00005 的区块 E，采用预设的散列算法将备份节点针对标识信息 00005 的区块保存的每个备份数字证书进行散列运算，判断自身区块 E 中保存的每个数字证书是否均与散列运算后的备份数字证书对应匹配，如果对应匹配，确定所述备份节点针对区块 E 保存的每个备份数字证书未被篡改，每个备份数字证书正确，根据自身区块 E 中保存的数字证书 8 的状态信息为吊销、数字证书 9 的状态信息为未吊销，与数字证书 8 对应匹配的备份数字证书 8 的有效期为 2016 年 7 月 5 日-2017 年 7 月 5 日、与数字证书 9 对应匹配的备份数字证书 9 的有效期为 2015 年 8 月 5 日-2016 年 8 月 5 日，当前时间为 2017 年 3 月 29 日，确定数字证书 8 的状态信息为吊销，与数

字证书 9 对应匹配的备份数字证书 9 的有效期过期，确定自身区块 E 中保存的每个数字证书均无效。

实施例 7:

图 5 为本公开实施例提供的一种基于区块链的数字证书删除装置结构示意图，该装置包括:

确定模块 51，配置为根据自身针对每个区块保存的每个备份数字证书的信息，确定针对该区块保存的每个备份数字证书是否均无效;

发送模块 52，配置为如果确定针对该区块保存的每个备份数字证书均无效，向区块链中的每个验证节点发送包含该区块的标识信息的删除消息，使每个验证节点判断自身该标识信息的区块中每个数字证书是否均无效，并在确定该标识信息的区块中每个数字证书均无效时，删除该标识信息的区块的区块体。

所述确定模块 51，配置为根据自身针对每个区块保存的每个备份数字证书的信息，确定针对该区块保存的每个备份数字证书的有效期是否过期和/或备份数字证书是否已吊销；如果针对该区块保存的每个备份数字证书为有效期过期和/或备份数字证书已吊销，确定针对该区块保存的每个备份数字证书均无效。

所述发送模块 52，还配置为如果所述区块链中的每个验证节点的每个区块中保存的每个数字证书使用预设的算法进行变换，将自身针对所述标识信息的区块保存的每个备份数字证书发送给每个验证节点。

在本公开实施例中，如图 5 所示的基于区块链的数字证书删除装置，应用于区块链中的任一备份节点，其中所述区块链中包含多个验证节点和至少一个备份节点。

实施例 8:

图 6 为本公开实施例提供的一种基于区块链的数字证书删除装置结构

示意图，该装置包括:

接收模块 61，配置为接收区块链中备份节点发送的包含区块的标识信息的删除消息，其中所述删除消息为区块链中的备份节点根据其自身针对每个区块保存的每个备份数字证书的信息，确定针对该区块保存的每个备份数字证书均无效后发送的;

判断模块 62，配置为判断自身保存的该标识信息的区块中每个数字证书是否均无效;

删除模块 63，配置为如果确定该标识信息的区块中每个数字证书均无效，删除该区块的区块体。

所述接收模块 61，还配置为如果对每个区块保存的每个数字证书使用预设的算法进行变换，接收所述备份节点发送的所述备份节点针对所述标识信息的区块保存的每个备份数字证书;

所述装置还包括:

匹配模块 64，配置为采用所述预设的算法对所述每个备份数字证书进行变换；针对所述标识信息的区块中保存的每个数字证书，判断自身保存的每个数字证书是否均与该备份数字证书变换后的数字证书对应匹配；如果匹配结果为是，触发判断模块。

所述判断模块 62，配置为获取自身保存的该标识信息的区块中每个数字证书的有效期及状态信息；判断该标识信息的区块中每个数字证书的有效期是否过期和/或数字证书是否已吊销；如果该标识信息的区块中每个数字证书为有效期过期和/或数字证书的状态为吊销，确定该标识信息的区块中每个数字证书均无效。

在本公开实施例中，如图 6 所示的基于区块链的数字证书删除装置，应用于区块链中的任一验证节点，其中所述区块链中包含多个验证节点和至少一个备份节点。

实施例 9:

图 7 为本公开实施例实施例提供的一种基于区块链的数字证书删除系统结构示意图，该删除系统包括至少一个应用于备份节点 71 的基于区块链的数字证书删除装置，及多个应用于验证节点 72 的基于区块链的数字证书删除装置。

本公开实施例公开了一种基于区块链的数字证书删除方法、装置及系统，所述区块链中包含多个验证节点和至少一个备份节点，所述删除方法应用于区块链中的任一备份节点，所述方法包括：根据自身针对每个区块保存的每个备份数字证书的信息，确定针对该区块保存的每个备份数字证书是否均无效；如果确定针对该区块保存的每个备份数字证书均无效，向区块链中的每个验证节点发送包含该区块的标识信息的删除消息，使每个验证节点判断自身该标识信息的区块中每个数字证书是否均无效，并在确定该标识信息的区块中每个数字证书均无效时，删除该标识信息的区块的区块体。由于在本公开实施例中，如果备份节点判断针对某一区块保存的每个备份数字证书均无效，向区块链中的每个验证节点发送包含该区块的标识信息的删除消息，使每个验证节点判断自身该标识信息的区块中每个数字证书是否均无效，并在确定该标识信息的区块中每个数字证书均无效时，删除该标识信息的区块的区块体，减少了数据证书存储过程中占用的存储空间，节约了验证节点的存储和计算资源，提高了验证节点的运行效率和用户的体验。

对于系统/装置实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

本公开实施例还公开了一种计算机存储介质，所述计算机存储介质存储有计算可执行指令；所述计算机可执行指令被执行后，能够实现应用于备份节点的基于区块链的数字证书删除方法中的一个或多个，或实现应用

于验证节点的基于区块链的数字证书删除方法中的一个或多个，例如，执行如图 2 和/或图 4 所示的方法。本申请实施例中提到的计算机存储介质可为各种类型的存储介质，可选为非瞬间存储介质。

本领域内的技术人员应明白，本申请的实施例可提供为方法、系统、或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

本申请是参照根据本申请实施例的方法、设备（系统）、和计算机程序产品的流程图和／或方框图来描述的。应理解可由计算机程序指令实现流程图和／或方框图中的每一流程和／或方框、以及流程图和／或方框图中的流程和／或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能的装置。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能。

这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的

功能的步骤。

尽管已描述了本申请的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例做出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本申请范围的所有变更和修改。

显然，本领域的技术人员可以对本公开实施例进行各种改动和变型而不脱离本公开实施例的精神和范围。这样，倘若本公开实施例的这些修改和变型属于本公开实施例权利要求及其等同技术的范围之内，则本公开实施例也意图包含这些改动和变型在内。

工业实用性

本公开实施例中若一个备份节点发现自身存储的一个区域上的所有备份数字证书中的每个备份数字证书均无效时，会生成删除消息，从而可以使得所有存储该区块的验证节点至少可以删除该区块的区块体，一方面减少存储的数据量，从而减少所消耗的存储资源，另一方面减少后续区块链在生成过程中的校验数据量，从而节省校验所需的计算资源，提升校验效率，故具有积极的工业效果。与此同时，本公开实施例提供的技术方案具有实现简便的特点，可在工业上广泛实施。

权利要求书

1、一种基于区块链的数字证书删除方法，所述区块链中包含多个验证节点和至少一个备份节点，所述删除方法应用于区块链中的任一备份节点，所述方法包括:

根据自身针对每个区块保存的每个备份数字证书的信息，确定针对该区块保存的每个备份数字证书是否均无效;

如果确定针对该区块保存的每个备份数字证书均无效，向区块链中的每个验证节点发送包含该区块的标识信息的删除消息，其中，所述删除消息，用于使每个验证节点判断自身该标识信息的区块中每个数字证书是否均无效，并在确定该标识信息的区块中每个数字证书均无效时，删除该标识信息的区块的区块体。

2、如权利要求 1 所述的方法，其中，所述根据自身针对每个区块保存的每个备份数字证书的信息，确定针对该区块保存的每个备份数字证书是否均无效包括:

根据自身针对每个区块保存的每个备份数字证书的信息，确定针对该区块保存的每个备份数字证书的有效期是否过期和/或备份数字证书是否已吊销;

如果针对该区块保存的每个备份数字证书为有效期过期和/或备份数字证书已吊销，确定针对该区块保存的每个备份数字证书均无效。

3、如权利要求 1 所述的方法，其中，如果所述区块链中的每个验证节点的每个区块中保存的每个数字证书使用预设的算法进行变换，所述向区块链中的每个验证节点发送包含该区块的标识信息的删除消息后，所述方法还包括:

将自身针对所述标识信息的区块保存的每个备份数字证书发送给每个

验证节点。

4、一种基于区块链的数字证书删除方法，所述区块链中包含多个验证节点和至少一个备份节点，所述删除方法应用于区块链中的任一验证节点，所述方法包括:

接收区块链中备份节点发送的包含区块的标识信息的删除消息，其中所述删除消息为：区块链中的备份节点根据其自身针对每个区块保存的每个备份数字证书的信息，确定针对该区块保存的每个备份数字证书均无效后发送的;

判断自身保存的该标识信息的区块中每个数字证书是否均无效;

如果确定该标识信息的区块中每个数字证书均无效，删除该区块的区块体。

5、如权利要求 4 所述的方法，其中，如果对每个区块保存的每个数字证书使用预设的算法进行变换，所述接收区块链中备份节点发送的包含区块的标识信息的删除消息后，所述方法还包括:

接收所述备份节点发送的所述备份节点针对所述标识信息的区块保存的每个备份数字证书;

所述方法还包括:

采用所述预设的算法对所述每个备份数字证书进行变换;

针对所述标识信息的区块中保存的每个数字证书，判断自身保存的每个数字证书是否均与该备份数字证书变换后的数字证书对应匹配;

所述判断自身保存的该标识信息的区块中每个数字证书是否均无效，包括:

如果自身保存的每个数字证书均与该备份数字证书变换后的数字证书对应匹配，判断自身保存的该标识信息的区块中每个数字证书是否均无效。

6、如权利 4 或 5 所述的方法，其中，所述判断自身保存的该标识信息

的区块中每个数字证书是否均无效包括:

获取自身保存的该标识信息的区块中每个数字证书的有效期及状态信息;

判断该标识信息的区块中每个数字证书的有效期是否过期和/或数字证书是否已吊销;

如果该标识信息的区块中每个数字证书为有效期过期和/或数字证书的状态为吊销，确定该标识信息的区块中每个数字证书均无效。

7、一种基于区块链的数字证书删除装置，所述装置包括:

确定模块，配置为根据自身针对每个区块保存的每个备份数字证书的信息，确定针对该区块保存的每个备份数字证书是否均无效;

发送模块，配置为如果确定针对该区块保存的每个备份数字证书均无效，向区块链中的每个验证节点发送包含该区块的标识信息的删除消息，使每个验证节点判断自身该标识信息的区块中每个数字证书是否均无效，并在确定该标识信息的区块中每个数字证书均无效时，删除该标识信息的区块的区块体。

8、如权利要求 7 所述的装置，其中，所述确定模块，配置为根据自身针对每个区块保存的每个备份数字证书的信息，确定针对该区块保存的每个备份数字证书的有效期是否过期和/或备份数字证书是否已吊销；如果针对该区块保存的每个备份数字证书为有效期过期和/或备份数字证书已吊销，确定针对该区块保存的每个备份数字证书均无效。

9、如权利要求 7 所述的装置，其中，所述发送模块，还配置为如果所述区块链中的每个验证节点的每个区块中保存的每个数字证书使用预设的算法进行变换，将自身针对所述标识信息的区块保存的每个备份数字证书发送给每个验证节点。

10、一种基于区块链的数字证书删除装置，所述装置包括:

接收模块，配置为接收区块链中备份节点发送的包含区块的标识信息的删除消息，其中所述删除消息为区块链中的备份节点根据其自身针对每个区块保存的每个备份数字证书的信息，确定针对该区块保存的每个备份数字证书均无效后发送的；

判断模块，配置为判断自身保存的该标识信息的区块中每个数字证书是否均无效；

删除模块，配置为如果确定该标识信息的区块中每个数字证书均无效，删除该区块的区块体。

11、如权利要求 10 所述的装置，其中，所述接收模块，还配置为于如果对每个区块保存的每个数字证书使用预设的算法进行变换，接收所述备份节点发送的所述备份节点针对所述标识信息的区块保存的每个备份数字证书；

所述装置还包括:

匹配模块，配置为采用所述预设的算法对所述每个备份数字证书进行变换；针对所述标识信息的区块中保存的每个数字证书，判断自身保存的每个数字证书是否均与该备份数字证书变换后的数字证书对应匹配；如果匹配结果为是，触发判断模块。

12、如权利要求 10 所述的装置，其中，所述判断模块，配置为获取自身保存的该标识信息的区块中每个数字证书的有效期及状态信息；判断该标识信息的区块中每个数字证书的有效期是否过期和/或数字证书是否已吊销；如果该标识信息的区块中每个数字证书为有效期过期和/或数字证书的状态为吊销，确定该标识信息的区块中每个数字证书均无效。

13、一种基于区块链的数字证书删除系统，其中，所述删除系统包括至少一个如权利要求 7-9 任一项所述的应用于备份节点的基于区块链的数字证书删除装置，及多个如权利要求 10-12 任一项所述的应用于验证

节点的基于区块链的数字证书删除装置。

14、一种计算机存储介质，所述计算机存储介质存储有计算可执行指令；所述计算机可执行指令被执行后，能够实现权利要求 1-3 或 4-6 任一项提供的基于区块链的数字证书删除方法。

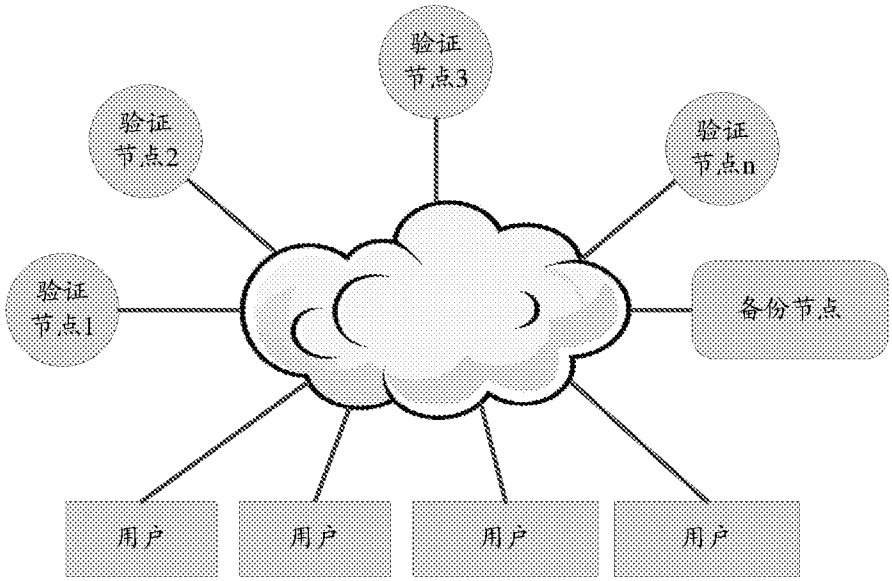
验证
节点3
验证
节点2
验证
节点n
验证
节点1
备份节点
用户
用户
用户
用户

图 1

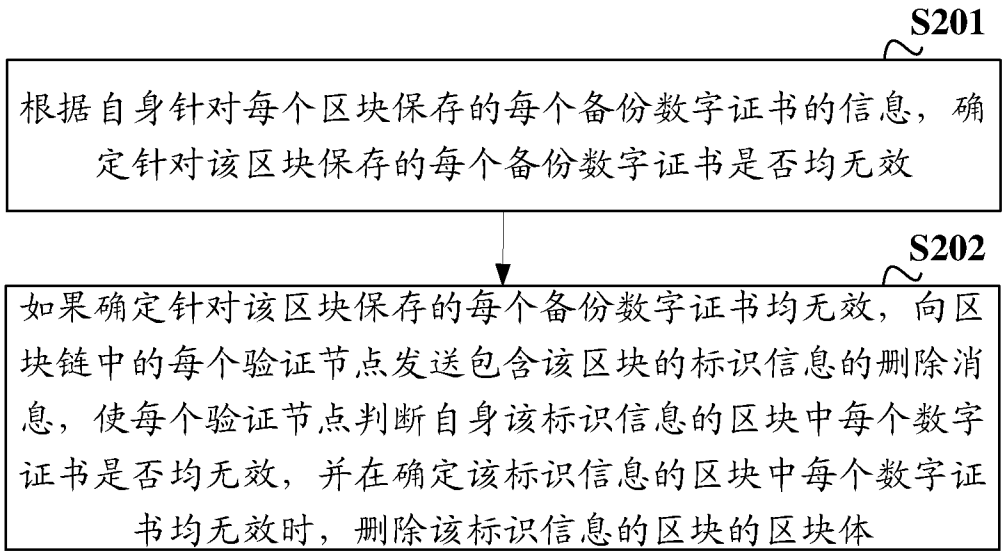
S201
根据自身针对每个区块保存的每个备份数字证书的信息，确定针对该区块保存的每个备份数字证书是否均无效
S202
如果确定针对该区块保存的每个备份数字证书均无效，向区块链中的每个验证节点发送包含该区块的标识信息的删除消息，使每个验证节点判断自身该标识信息的区块中每个数字证书是否均无效，并在确定该标识信息的区块中每个数字证书均无效时，删除该标识信息的区块的区块体

图 2

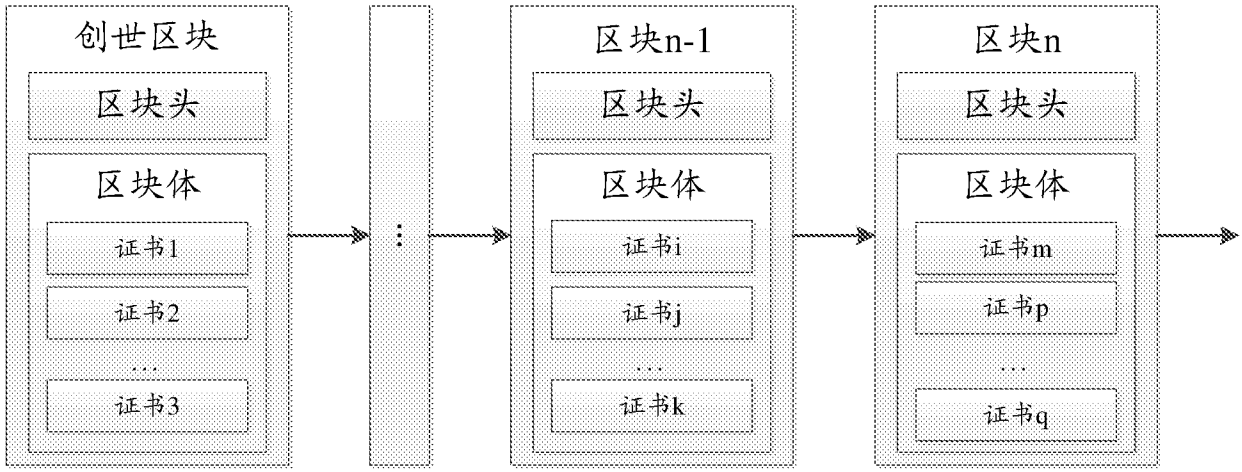
创世区块
区块头
区块体
证书1
证书2
...
证书3
区块n-1
区块头
区块体
证书i
证书j
...
证书k
区块n
区块头
区块体
证书m
证书p
...
证书q

图 3

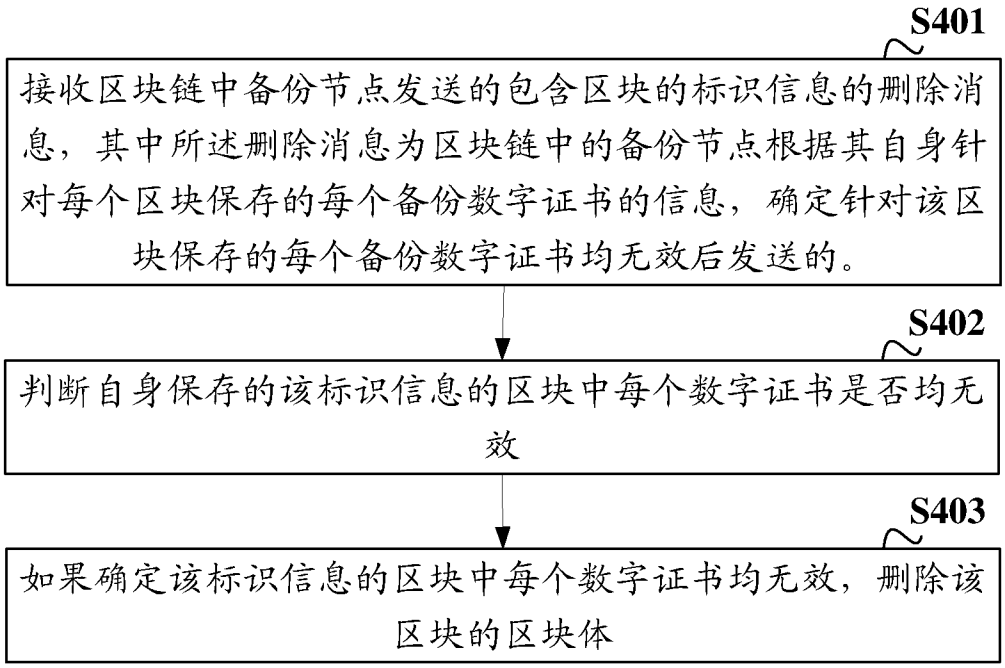
S401
接收区块链中备份节点发送的包含区块的标识信息的删除消息，其中所述删除消息为区块链中的备份节点根据其自身针对每个区块保存的每个备份数字证书的信息，确定针对该区块保存的每个备份数字证书均无效后发送的。
S402
判断自身保存的该标识信息的区块中每个数字证书是否均无效
S403
如果确定该标识信息的区块中每个数字证书均无效，删除该区块的区块体

图 4

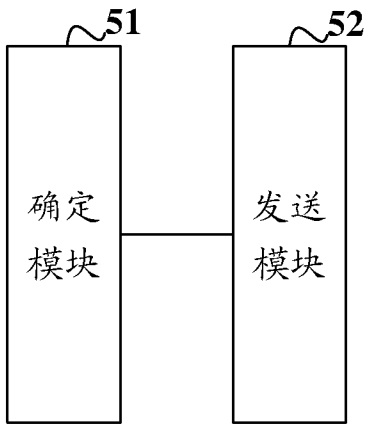

图 5

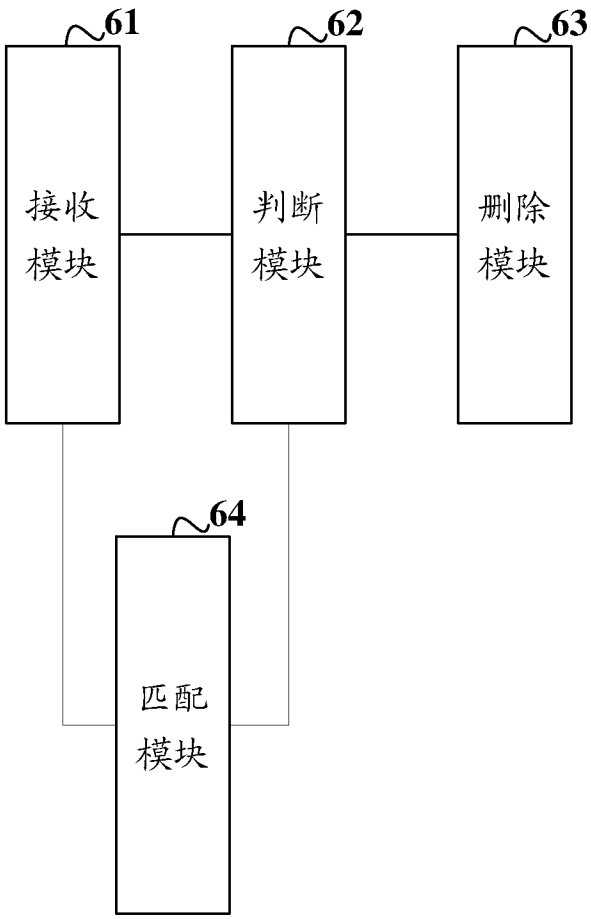

图 6

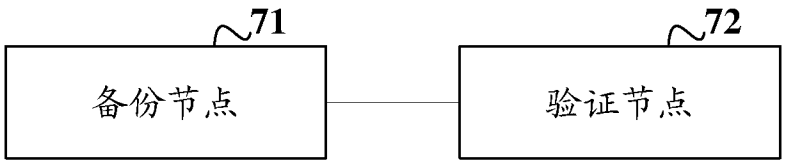

图 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2018/078888

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; USTXT; WOTXT; EPTXT; CNKI: 区块链, 区块, 证书, 删除, 备份, 节点, 无效, 过期, blockchain, block, certificate, delete, backup, node, invalid, expire

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 106385315 A (BEIJING SANSEC TECHNOLOGY DEVELOPMENT CO., LTD.) 08 February 2017 (08.02.2017), description, paragraphs [0075]-[0101]	1-14
A	CN 105790954 A (BUBI (BEIJING) NETWORK TECHNOLOGY CO., LTD.) 20 July 2016 (20.07.2016), entire document	1-14
A	US 2015206106 A1 (YAGO YARON EDAN) 23 July 2015 (23.07.2015), entire document	1-14

☐ 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
28 April 2018	01 June 2018
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer DING, Xiao Telephone No. (86-512) 88996052

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2018/078888

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 106385315 A	08 February 2017	None	
CN 105790954 A	20 July 2016	None	
US 2015206106 A1	23 July 2015	WO 2015106285 A1	16 July 2015

国际检索报告

国际申请号
PCT/CN2018/078888

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;USTXT;WOTXT;EPTXT;CNKI：区块链，区块，证书，删除，备份，节点，无效，过期，blockchain，block，certificate，delete，backup，node，invalid，expire

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
A	CN 106385315 A (北京三未信安科技发展有限公司) 2017年 2月 8日 (2017-02-08) 说明书第[0075]-[0101]段	1-14
A	CN 105790954 A (布比北京网络技术有限公司) 2016年 7月 20日 (2016-07-20) 全文	1-14
A	US 2015206106 A1 (YAGO YARON EDAN) 2015年 7月 23日 (2015-07-23) 全文	1-14

☐ 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
2018年 4月 28日	2018年 6月 1日
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局(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 丁筱 电话号码 86-(512)-88996052

表 PCT/ISA/210 (第2页) (2015年1月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2018/078888

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 106385315 A	2017年 2月 8日	无	
CN 105790954 A	2016年 7月 20日	无	
US 2015206106 A1	2015年 7月 23日	WO 2015106285 A1	2015年 7月 16日