(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
2021 年 4 月 15 日 (15.04.2021)

WIPO | PCT

(10) 国际公布号
WO 2021/068636 A1

(51) 国际专利分类号:
G06F 16/27 (2019.01) *G06Q 30/00* (2012.01)

(21) 国际申请号: PCT/CN2020/107903

(22) 国际申请日: 2020 年 8 月 7 日 (07.08.2020)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910963431.0 2019年10月11日 (11.10.2019) CN

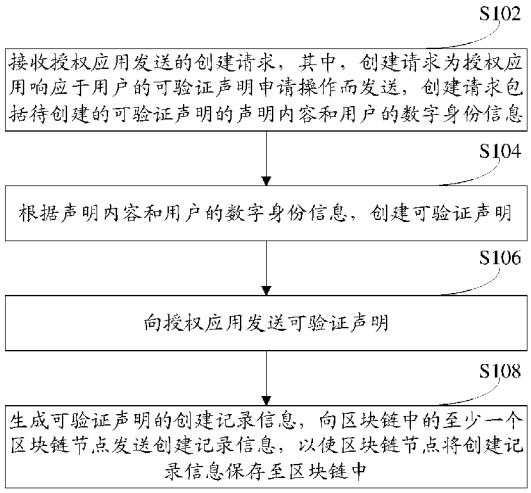
(71) 申请人: 支付宝（杭州）信息技术有限公司 (ALIPAY (HANGZHOU) INFORMATION TECHNOLOGY CO., LTD.) [CN/CN]; 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。

(72) 发明人: 刘佳伟 (LIU, Jiawei); 中国浙江省杭州市西湖区西溪路556号8层B段801-11, Zhejiang 310000 (CN)。 孙善禄 (SUN, Shanlu); 中国浙江省杭州市西湖区西溪路556号8层B段801-11, Zhejiang 310000 (CN)。 代平 (DAI, Ping); 中国浙江省杭州市西湖区西溪路556号8层B段801-11, Zhejiang 310000 (CN)。 刘丹 (LIU, Dan); 中国浙江省杭州市西湖区西溪路556号8层B段801-11, Zhejiang 310000 (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)。

(54) **Title:** BLOCK CHAIN-BASED CREATION METHOD, APPARATUS, DEVICE AND SYSTEM FOR VERIFIABLE CLAIM

(54) **发明名称**: 基于区块链的可验证声明的创建方法、装置、设备及系统



S102 Receive a creation request sent by an authorization application, the creation request being sent by the authorization application in response to a verifiable claim application operation of a user, the creation request containing claim content of a verifiable claim to be created and decentralized identity of the user

S104 Create a verifiable claim according to the claim content and the decentralized identity of the user

S106 Send the verifiable claim to the authorization application

S108 Generate creation record information of the verifiable claim, and send the creation record information to at least one block chain node in a block chain, so that the block chain node saves the creation record information in the block chain

图 2

(57) **Abstract:** A block chain-based creation method, apparatus, device and system for a verifiable claim. Said method comprises: in response to a verifiable claim application operation of a user, an authorization application sending a creation request to a creation platform; the creation platform creating a verifiable claim according to claim content and decentralized identity of the user contained in the creation request, and sending the verifiable claim to the authorization application; and generating creation record information of the verifiable claim, and sending the creation record information to at least one block chain node in a block chain, so that the block chain node saves the creation record information in the block chain.

(57) **摘要**: 一种基于区块链的可验证声明的创建方法、装置、设备及系统，其中方法包括：授权应用响应于用户的可验证声明申请操作，发送创建请求给创建平台；创建平台根据创建请求包括的声明内容和用户的数字身份信息，创建可验证声明，向授权应用发送所述可验证声明；以及，生成可验证声明的创建记录信息，向区块链中的至少一个区块链节点发送创建记录信息，以使区块链节点将创建记录信息保存至区块链中。

WO 2021/068636 A1

[见续页]

(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, IT, 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, 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))。

基于区块链的可验证声明的创建方法、装置、设备及系统

技术领域

[01] 本文件涉及数字身份技术领域，尤其涉及一种基于区块链的可验证声明的创建方法、装置、设备及系统。

背景技术

[02] 生活中人们常常遇到一些需要证明自己的场景，例如在银行办理开户业务或者参与某个重要活动时，需要使用有效的身份证件来证明自己的身份，又如在办理入职手续或者办理与学业相关的业务时，需要使用已有的毕业证来证明自己当前的学历等。然而，诸如身份证、毕业证等实体证件，人们通常不会随身携带，因而避免不了的会因忘记携带证件而影响业务的正常办理。

发明内容

[03] 本说明书一个或多个实施例提供了一种基于区块链的可验证声明的创建方法，应用于可验证声明的创建平台。该创建方法包括接收授权应用发送的创建请求，其中，所述创建请求为所述授权应用响应于用户的可验证声明申请操作而发送，所述创建请求包括待创建的可验证声明的声明内容和所述用户的数字身份信息。根据所述声明内容和所述数字身份信息，创建可验证声明，向所述授权应用发送所述可验证声明。生成所述可验证声明的创建记录信息，向区块链中的至少一个区块链节点发送所述创建记录信息，以使所述区块链节点将所述创建记录信息保存至区块链中。

[04] 本说明书一个或多个实施例提供了一种可验证声明的创建方法，应用于授权应用。该方法包括响应于用户的可验证声明申请操作，获取待创建的可验证声明的声明内容，根据所述声明内容和所述用户的数字身份信息，向创建平台发送创建请求，以使所述创建平台根据所述声明内容和所述用户的数字身份信息创建可验证声明，接收所述创建平台发送的所述可验证声明。

[05] 本说明书一个或多个实施例提供了一种基于区块链的可验证声明的创建方法，应用于区块链中的区块链节点。该方法包括接收创建平台发送的可验证声明的创建记录信息，其中，所述创建记录信息为所述创建平台根据授权应用发送的创建请求，创建所述可验证声明之后所生成的信息；将所述创建记录信息保存至区块链中。

[06] 本说明书一个或多个实施例提供了一种基于区块链的可验证声明的创建装置，应用于可验证声明的创建平台。该创建装置包括接收模块，其接收授权应用发送的创建请求，其中，所述创建请求为所述授权应用响应于用户的可验证声明申请操作而发送，所述创建请求包括：待创建的可验证声明的声明内容和所述用户的数字身份信息。该创建装置还包括创建模块，其根据所述声明内容和所述数字身份信息，创建可验证声明。该创建装置还包括发送模块，其向所述授权应用发送所述可验证声明。该创建装置还包括生成模块，其生成所述可验证声明的创建记录信息，向区块链中的至少一个区块链节点发送所述创建记录信息，以使所述区块链节点将所述创建记录信息保存至区块链中。

[07] 本说明书一个或多个实施例提供了一种可验证声明的创建装置，应用于授权应用。该创建装置包括获取模块，其响应于用户的可验证声明申请操作，获取待创建的可验证声明的声明内容。该创建装置还包括发送模块，其根据所述声明内容和所述用户的数字身份信息，向创建平台发送创建请求，以使所述创建平台根据所述声明内容和所述用户的数字身份信息，创建可验证声明。该创建装置还包括接收模块，其接收所述创建平台发送的所述可验证声明。

[08] 本说明书一个或多个实施例提供了一种基于区块链的可验证声明的创建装置，应用于区块链中的区块链节点。该创建装置包括接收模块，其接收创建平台发送的可验证声明的创建记录信息，其中，所述创建记录信息为所述创建平台根据授权应用发送的创建请求，创建所述可验证声明之后所生成的信息。该创建装置还保存模块，其将所述创建记录信息保存至区块链中。

[09] 本说明书一个或多个实施例提供了一种基于区块链的可验证声明的创建系统，包括授权应用、创建平台和区块链。所述授权应用，响应于用户的可验证声明申请操作，获取待创建的可验证声明的声明内容，根据所述声明内容和所述用户的数字身份信息，向所述创建平台发送创建请求。所述创建平台，根据所述声明内容和所述数字身份信息，创建可验证声明，向所述授权应用发送所述可验证声明。以及，生成所述可验证声明的创建记录信息，将所述创建记录信息发送给所述区块链中的至少一个区块链节点。所述区块链中的区块链节点，在接收到所述创建记录信息时，将所述创建记录信息保存至区块链中。

[10] 本说明书一个或多个实施例提供了一种基于区块链的可验证声明的创建设备，包括处理器。该创建设备还包括被安排成存储计算机可执行指令的存储器。所述计算机可执行指令在被执行时使所述处理器接收授权应用发送的创建请求，其中，所述创建请求

为所述授权应用响应于用户的可验证声明申请操作而发送，所述创建请求包括待创建的可验证声明的声明内容和所述用户的数字身份信息。根据所述声明内容和所述数字身份信息，创建可验证声明，向所述授权应用发送所述可验证声明。生成所述可验证声明的创建记录信息，向区块链中的至少一个区块链节点发送所述创建记录信息，以使所述区块链节点将所述创建记录信息保存至区块链中。

[11] 本说明书一个或多个实施例提供了一种可验证声明的创建设备，包括处理器。该创建设备还包括被安排成存储计算机可执行指令的存储器。所述计算机可执行指令在被执行时使所述处理器响应于用户的可验证声明申请操作，获取待创建的可验证声明的声明内容；根据所述声明内容和所述用户的数字身份信息，向创建平台发送创建请求，以使所述创建平台根据所述声明内容和所述用户的数字身份信息，创建可验证声明。接收所述创建平台发送的所述可验证声明。

[12] 本说明书一个或多个实施例提供了一种基于区块链的可验证声明的创建设备，包括处理器。该创建设备还包括被安排成存储计算机可执行指令的存储器。所述计算机可执行指令在被执行时使所述处理器接收创建平台发送的可验证声明的创建记录信息，其中，所述创建记录信息为所述创建平台根据授权应用发送的创建请求，创建所述可验证声明之后所生成的信息。将所述创建记录信息保存至区块链中。

[13] 本说明书一个或多个实施例提供了一种存储介质，用于存储计算机可执行指令。所述计算机可执行指令在被执行时接收授权应用发送的创建请求，其中，所述创建请求为所述授权应用响应于用户的可验证声明申请操作而发送，所述创建请求包括待创建的可验证声明的声明内容和所述用户的数字身份信息。根据所述声明内容和所述数字身份信息，创建可验证声明，向所述授权应用发送所述可验证声明。生成所述可验证声明的创建记录信息，向区块链中的至少一个区块链节点发送所述创建记录信息，以使所述区块链节点将所述创建记录信息保存至区块链中。

[14] 本说明书一个或多个实施例提供了一种存储介质，用于存储计算机可执行指令。所述计算机可执行指令在被执行时响应于用户的可验证声明申请操作，获取待创建的可验证声明的声明内容。根据所述声明内容和所述用户的数字身份信息，向创建平台发送创建请求，以使所述创建平台根据所述声明内容和所述用户的数字身份信息，创建可验证声明。接收所述创建平台发送的所述可验证声明。

[15] 本说明书一个或多个实施例提供了一种存储介质，用于存储计算机可执行指令，所述计算机可执行指令在被执行时接收创建平台发送的可验证声明的创建记录信息，其

中，所述创建记录信息为所述创建平台根据授权应用发送的创建请求，创建所述可验证声明之后所生成的信息。将所述创建记录信息保存至区块链中。

附图说明

[16] 为了更清楚地说明本说明书一个或多个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中记载的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[17] 图 1 为本说明书一个或多个实施例提供的一种基于区块链的可验证声明的创建方法的场景示意图。

[18] 图 2 为本说明书一个或多个实施例提供的一种基于区块链的可验证声明的创建方法的第一种流程示意图。

[19] 图 3 为本说明书一个或多个实施例提供的一种基于区块链的可验证声明的创建方法的第二中流程示意图。

[20] 图 4 为本说明书一个或多个实施例提供的生成创建记录信息的流程示意图。

[21] 图 5 为本说明书一个或多个实施例提供的一种可验证声明的创建方法的流程示意图。

[22] 图 6 为本说明书一个或多个实施例提供的一种基于区块链的可验证声明的创建方法的第三种流程示意图。

[23] 图 7 为本说明书一个或多个实施例提供的验证可验证声明的第一种流程示意图。

[24] 图 8 为本说明书一个或多个实施例提供的验证可验证声明的第二种流程示意图。

[25] 图 9 为本说明书一个或多个实施例提供的一种基于区块链的可验证声明的创建装置的第一种模块组成示意图。

[26] 图 10 为本说明书一个或多个实施例提供的一种可验证声明的创建装置的模块组成示意图。

[27] 图 11 为本说明书一个或多个实施例提供的一种基于区块链的可验证声明的创建装置的第二种模块组成示意图。

[28] 图 12 为本说明书一个或多个实施例提供的一种基于区块链的可验证声明的创建系

统的组成示意图。

[29] 图 13 为本说明书一个或多个实施例提供的一种基于区块链的可验证声明的创建设备的结构示意图。

[30] 图 14 为本说明书一个或多个实施例提供的一种可验证声明的创建设备的结构示意图。

具体实施方式

[31] 为了使本技术领域的人员更好地理解本说明书一个或多个实施例中的技术方案，下面将结合本说明书一个或多个实施例中的附图，对本说明书一个或多个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。基于本说明书一个或多个实施例，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，都应当属于本文件的保护范围。

[32] 图 1 为本说明书一个或多个实施例提供的基于区块链的可验证声明的创建方法的应用场景示意图，如图 1 所示，该场景包括：用户的终端设备、可验证声明的创建平台和区块链中的至少一个区块链节点（图 1 中仅示出一个）；其中，用户的终端设备中安装有授权应用，用户可以操作该授权应用向创建平台申请可验证声明，用户的终端设备可以为手机、平板电脑、台式计算机、便携笔记本式计算机等；创建平台可以为具有可验证声明的创建权限的权威机构，创建平台通过无线网络与用户的终端设备和区块链节点进行通讯连接。

[33] 具体的，用户操作其终端设备中的授权应用，编辑声明内容等信息，并在编辑完成时，操作（如单击或双击）授权应用中的控件（如提交控件），以向授权应用发送可验证声明的申请请求；授权应用响应于用户的可验证声明申请操作，获取待创建的可验证声明的声明内容；根据声明内容和用户的数字身份信息（英文全称：Decentralized Identity，英文简称：DID），向创建平台发送创建请求；创建平台接收授权应用发送的创建请求，根据创建请求包括的声明内容和用户的数字身份信息，创建可验证声明；创建平台向授权应用发送创建的可验证声明，并生成可验证声明的创建记录信息，向区块链中的至少一个区块链节点发送创建记录信息；授权应用接收创建平台发送的可验证声明；区块链节点将接收到的创建记录信息保存至区块链中。

[34] 其中，声明内容包括声明信息、可验证声明的有效截止时间，还可以包括安全机

制信息、可验证声明的隐匿属性等；声明信息如学历、年龄、资产（如房产）等，对应的，可验证声明用于证明用户的学历、年龄、所拥有的资产等；安全机制信息表征在基于可验证声明办理业务时，是否需要向用户进行业务办理确认；隐匿属性表征可验证声明是否公开。

[35] 用户的数字身份信息和创建平台的数字身份信息，分别由用户和创建平台预先从指定平台申请而得。例如，用户从指定平台申请数字身份信息时，用户操作其终端设备中安装的授权应用或者其他具有数字身份信息申请功能的应用，向指定平台发送数字身份信息申请请求，指定平台代理用户申请公私钥对，并根据其中的公钥生成数字身份信息，以及生成用户的数字身份信息对应的文档（DID doc），将生成的数字身份信息发送给对应的应用，并将公钥、加密协议等相关信息保存至生成的文档中；又如，用户操作其终端设备中安装的授权应用或者其他具有数字身份信息申请功能的应用，向指定平台发送数字身份信息申请请求，其中，数字身份信息申请请求中包括用户的身份证件号码等信息，指定平台在对用户进行实人认证（如刷脸认证、指纹认证等）之后，根据用户的身份证件号码生成用户的数字身份信息，以及生成用户的数字身份信息对应的文档，将生成的数字身份信息发送给对应的应用，并获取用户的与数字身份信息对应的公钥，将获取的公钥及其他相关信息保存至生成的文档中；需要指出的是，创建平台申请数字身份信息的过程可参见用户申请数字身份信息的过程，重复之处不再赘述；并且对于数字身份信息的申请过程，本说明书中不做具体限定，其可在实际应用中根据需要自行设定。

[36] 上述应用场景中，通过创建可验证声明，并将创建记录信息保存至区块链上，使得用户可以基于该可验证声明，在办理相关业务时证明自己，而无需准备相应的实体文件（如身份证），为用户提供了便利；同时，对于业务提供方而言，能够通过区块链节点基于区块链中存储的创建记录信息对用户提供的可验证声明进行验证，不仅确保了业务安全，而且无需对实体文件进行目检，提升了验证效率和验证的准确率。

[37] 基于上述应用场景架构，本说明书一个或多个实施例提供了一种基于区块链的可验证声明的创建方法；图 2 为本说明书一个或多个实施例提供的一种基于区块链的可验证声明的创建方法的流程示意图，图 2 中的方法能够由图 1 中的服务端执行，如图 2 所示，该方法包括步骤 S102-S108。

[38] 步骤 S102，接收授权应用发送的创建请求，其中，创建请求为授权应用响应于用户的可验证声明申请操作而发送，创建请求包括待创建的可验证声明的声明内容和用户

的数字身份信息。

[39] 步骤 S104，根据声明内容和用户的数字身份信息，创建可验证声明。

[40] 步骤 S106，向授权应用发送可验证声明。

[41] 步骤 S108，生成可验证声明的创建记录信息，向区块链中的至少一个区块链节点发送创建记录信息，以使区块链节点将创建记录信息保存至区块链中。

[42] 本说明书一个或多个实施例中，通过创建可验证声明，并将创建记录信息保存至区块链上，使得用户可以基于该可验证声明，在办理相关业务时证明自己，而无需准备相应的实体文件（如身份证），为用户提供了便利；同时，对于业务提供方而言，能够通过区块链节点基于区块链中存储的创建记录信息对用户提供的可验证声明进行验证，不仅确保了业务安全，而且无需对实体文件进行目检，提升了验证效率和验证的准确率。

[43] 为了使用户在基于可验证声明办理业务时，无需提供与可验证声明相关的额外的信息，如可验证声明的创建方的信息等；本说明书一个或多个实施例中，将创建平台的数字身份信息、用户的数字身份信息、声明内容以及所需的更多的字段信息均记载于可验证声明中，具体的，如图 3 所示，步骤 S104 包括 S104-2 和 S104-4。

[44] 步骤 S104-2，确定创建所述可验证声明所需的字段信息。

[45] 步骤 S104-4，根据确定的字段信息、声明内容、用户的数字身份信息及创建平台的数字身份信息，创建可验证声明。

[46] 为了对不同的可验证声明进行有效区分，以及在业务提供方接收到用户提供的可验证声明时，可以对可验证声明进行多方面的有效性验证，本说明书一个或多个实施例中，步骤 S104-2 包括步骤 S104-2-2~S104-2-6。

[47] 步骤 S104-2-2，生成可验证声明的声明标识；具体的，根据预设的声明标识的生成机制，生成可验证声明的声明标；其中，预设的声明标识的生成机制，可以在实际应用中根据需要自行设定，例如对创建请求所包括的一个或多个信息进行计算，并将计算结果或者计算结果中的部分信息作为声明标识；或者根据预设的动态生成机制动态生成声明标识，其中，动态生成机制能够确保每次生成的声明标识均不同。

[48] 步骤 S104-2-4，采用创建平台的私钥对预设的第一指定信息进行签名，得到签名数据；其中，第一指定信息可以为创建平台的数字身份信息，也可以为第一指定平台设定的某个信息，还可以为用户的数字身份信息、声明内容中的部分信息或全部信息等，

本说明书中对第一指定信息的具体内容不做具体限定。

[49] 进一步的，创建平台的私钥可以由创建平台自行保管，还可以由托管平台代理创建平台保管，并在创建平台需要使用其私钥时从托管平台获取；与之对应的，步骤S104-2-4 包括:

[50] 确定创建平台是否存储有私钥；若是，则采用创建平台存储的私钥对预设的第一指定信息进行签名，得到签名数据；若否，则从托管平台获取创建平台的私钥，并采用获取的私钥对预设的第一指定信息进行签名，得到签名数据。

[51] 如前述描述的数字身份信息的申请过程中会确定数字身份信息对应的公私钥，因此步骤 S104-2-4 包括: 确定创建平台是否存储有与创建平台的数字身份信息对应的私钥；若是，则采用创建平台存储的与创建平台的数字身份信息对应的私钥对预设的第一指定信息进行签名，得到签名数据；若否，则从托管平台获取与创建平台的数字身份信息对应的私钥，并采用获取的私钥对预设的第一指定信息进行签名，得到签名数据。

[52] 步骤 S104-2-6，将声明标识和签名数据作为创建可验证声明所需的字段信息。

[53] 通过确定声明标识和签名数据，并根据该声明标识、签名数据、声明内容、用户的数字身份信息及创建平台的数字身份信息，创建可验证声明，使得不仅可以根据声明标识对可验证声明进行区分，而且可以根据该声明标识快速的在区块链中查找对应的记录信息；再者，在用户基于可验证声明办理业务，对可验证声明进行验证时，可以根据可验证声明中的创建平台的数字身份信息索引到对应的文档（DID doc），从该文档中获取创建平台的公钥，并采用获取的公钥对可验证声明中的签名数据进行验签操作；或者，根据可验证声明中的创建平台的数字身份信息发送公钥获取请求给指定平台或机构，接收指定平台或机构返回的公钥，并采用接收的公钥对可验证声明中的签名数据进行验签操作；从而确保可验证声明是由创建平台所创建，而非伪造。

[54] 由于不同的用户对其个人信息隐私性的要求不同，因此，用户在申请可验证声明时，还可以设置可验证声明的隐匿属性；当隐匿属性为非公开时，如图 4 所示，步骤 S108 中生成可验证声明的创建记录信息，包括步骤 A2~A8。

[55] 步骤 A2，计算用户的数字身份信息的哈希值。

[56] 步骤 A4，计算创建平台的数字身份信息的哈希值。

[57] 步骤 A6，计算可验证声明中第二指定信息的哈希值。

[58] 其中，第二指定信息可以为用户的数字身份信息、创建平台的数字身份信息、声明内容、声明标识和有效性字段，还可以为用户的数字身份信息、创建平台的数字身份信息、声明内容、声明标识和有效性字段中的任意一个或几个的组合；其中，有效性字段表征可验证声明所处的状态，如有效状态、无效状态。

[59] 需要指出的是，步骤 A2、步骤 A4、步骤 A6 的执行顺序可以彼此互换，哈希值的计算算法可以在实际中根据需要自行设定。

[60] 步骤 A8，将计算的各个哈希值、声明标识、有效性字段进行关联记录，并将记录的信息作为可验证声明的创建记录信息。

[61] 通过计算用户的数字身份信息、创建平台的数字身份信息以及第二指定信息的哈希值，并根据哈希值生成创建记录信息，有效的确保了用户的隐私数据的安全；同时，通过将创建记录信息保存至区块链中，能够在用户使用可验证声明办理业务时，基于区块链中的创建记录信息对用户提供的可验证声明进行更全面的验证，确保可验证声明的真实性和有效性，从而确保业务安全。

[62] 进一步的，当用户设置的隐匿属性为公开时，步骤 S108 中生成可验证声明的创建记录信息，包括：将可验证声明、用户的数字身份信息、创建平台的数字身份信息、声明标识和有效性字段进行关联记录，并将记录的信息作为可验证声明的创建记录信息；其中，有效性字段表征可验证声明所处的状态。

[63] 通过将可验证声明的明文保存至区块链中，能够在用户使用可验证声明办理业务时，基于区块链中的创建记录信息对用户提供的可验证声明的真实性和有效性进行更直接的验证，从而确保业务安全。

[64] 考虑到用户的数字身份信息存在被盗用的风险，因此当声明内容涉及金融、资产（如房产）等与用户利益密切相关的事项时，存在用户利益受到损害的风险，例如盗用者采用用户房产相关的可验证声明去银行抵押贷款，从而给用户造成经济损失；基于此，本说明书一个或多个实施例中，预先设定不同的声明内容所对应的可验证声明的安全等级，并在待创建的可验证声明的安全等级满足预设条件时，对用户进行身份验证，以确保安全；具体的，步骤 S104 包括 B2~B6。

[65] 步骤 B2，若根据声明内容，确定待创建的可验证声明所对应的安全等级满足预设条件，则向授权应用发送身份验证请求；其中，安全等级和预设条件均可以在实际应用中根据需要自行设定，本说明书中对此不做具体限定。例如，将安全等级划分为一级、

二级、三级、四级、五级，且安全性的高低为一级>二级>三级>四级>五级，预设条件为待创建的可验证声明所对应的安全等级大于三级时，需要进行身份验证。

[66] 步骤 B4，接收授权应用发送的用户的身份验证信息；其中，身份验证信息可以为生物特征信息，如人脸、指纹、虹膜等中的任意一个或多个，还可以为验证码形式的验证信息。

[67] 步骤 B6，若根据身份验证信息对用户的身份验证通过，则根据声明内容和数字身份信息，创建可验证声明。

[68] 具体的，若身份验证信息为生物特征信息，则将身份验证信息与指定机构的数据库存储的用户的身份信息进行匹配，若匹配成功，则确定对用户的身份验证通过，若匹配失败，则确定对用户的身份验证失败，并发送请求失败的请求结果给授权应用。其中，指定机构为可信的第三方机构，具有权威性和合法性，其数据库中存储有用户的身份信息，通过访问该数据库，以对用户的身份验证信息进行认证；指定机构例如为公安局。若身份验证信息为验证码，则将授权应用发送的验证码与自身存储的验证码进行匹配，若匹配成功，则确定对用户的身份验证通过，若匹配失败，则确定对用户的身份验证失败，并发送请求失败的请求结果给授权应用。通过对用户进行身份验证，避免了因用户的数字身份信息被盗用而给用户造成的利益损失，提升了安全性。

[69] 在实际应用中，用户还可以操作其授权应用冻结、撤销其已申请的可验证声明，例如用户为了避免其可验证声明被盗用，在用户确定某一段时间内将不再使用可验证声明时，可以对其可验证声明进行冻结处理，使可验证声明处于无效状态，并在需要使用可验证声明时申请恢复其有效性；又如，用户可能因失误而提供了错误了声明内容，因此需要撤销对应的可验证声明等；基于此，本说明书一个或多个实施例中，所述方法还包括步骤 T2~T6。

[70] 步骤 T2，接收授权应用发送的声明处理请求，其中，声明处理请求包括待处理的可验证声明的声明标识；其中，声明处理请求用于请求对可验证声明进行冻结、解除冻结、撤销等处理。

[71] 步骤 T4，根据待处理的可验证声明的声明标识，表征可验证声明所处状态的有效性字段生成声明处理记录信息。

[72] 步骤 T6，向区块链中的至少一个区块链节点发送声明处理记录信息，以使区块链节点将声明处理记录信息保存至区块链中。

[73] 通过将声明处理记录信息保存至区块链中，能够在基于可验证声明办理业务时，为可验证声明的验证提供充分的验证依据，而且能够有效的避免因可验证声明被盗用而进行的非法业务操作。

[74] 本说明书一个或多个实施例中，通过创建可验证声明，并将创建记录信息保存至区块链上，使得用户可以基于该可验证声明，在办理相关业务时证明自己，而无需准备相应的实体文件（如身份证），为用户提供了便利；同时，对于业务提供方而言，能够基于区块链中存储的创建记录信息对用户提供的可验证声明进行验证，不仅确保了业务安全，而且无需对实体文件进行目检，提升了验证效率和验证的准确率。

[75] 对应上述图 2 至图 4 描述的可验证声明的创建方法，基于相同的技术构思，本说明书一个或多个实施例还提供一种可验证声明的创建方法，应用于授权应用；图 5 为本说明书一个或多个实施例提供的一种可验证声明的创建方法的流程示意图，如图 5 所示，该方法包括步骤 S202~S206。

[76] 步骤 S202，响应于用户的可验证声明申请操作，获取待创建的可验证声明的声明内容。具体而言，用户在申请可验证声明时，可以首先打开其终端设备中安装的授权应用，操作授权应用进入到可验证声明的申请界面，在该申请界面中编辑声明内容等信息，并在编辑完成时，操作（如单击或双击）申请界面中的提交控件，以发起可验证声明的申请请求；授权应用响应于用户的可验证声明申请操作，从该申请界面中获取待创建的可验证声明的声明内容。

[77] 步骤 S204，根据声明内容和用户的数字身份信息，向创建平台发送创建请求，以使创建平台根据声明内容和用户的数字身份信息，创建可验证声明。其中，用户的数字身份信息可以预先存储至授权应用中，也可以在用户申请可验证声明时，由用户自行编辑。

[78] 步骤 S206，接收创建平台发送的可验证声明。

[79] 进一步的，由于用户的数字身份信息存在被盗用的风险，因此当声明内容涉及金融、资产（如房产）等与用户利益密切相关的事项时，存在用户利益受到损害的风险；基于此，授权应用基于创建平台的身份验证请求，采集用户的身份验证信息以对用户进行身份验证；具体的，步骤 S206 之后还包括步骤 C2~C6。

[80] 步骤 C2，接收创建平台发送的身份验证请求。

[81] 步骤 C4，采集用户的身份验证信息。

[82] 步骤 C6，将采集的身份验证信息发送给创建平台，以使创建平台根据身份验证信息对用户的身份进行认证。

[83] 其中，身份验证信息可以为人脸、指纹、虹膜等中的任意一个或多个；以采集人脸为例，授权应用通过其所在终端设备的摄像头采集用户的人脸图像，并将采集的人脸图像发送给创建平台，以使创建平台根据该人脸图像对用户的身份进行认证。由此，通过对用户进行身份验证，避免了因用户的数字身份信息被盗用而给用户造成的利益损失，提升了安全性。

[84] 进一步的，用户还可以操作其授权应用对其已申请的可验证声明进行冻结、解除冻结、撤销等处理，对应的，方法还包括步骤 W2 和 W4。

[85] 步骤 W2，响应于用户的可验证声明处理操作，确定待处理的可验证声明的声明标识。

[86] 步骤 W4，根据待处理的可验证声明的声明标识，向创建平台发送声明处理请求，以使创建平台根据待处理的可验证声明的声明标识以及表征可验证声明所处状态的有效性字段，生成声明处理记录信息，并通过区块链节点将声明处理记录信息保存至区块链中。

[87] 由此，不仅能够在基于可验证声明进行业务处理时，为可验证声明的验证提供充分的验证依据，而且能够有效的避免因可验证声明被盗用而进行的非法业务操作。

[88] 本说明书一个或多个实施例中，授权应用响应于用户的可验证声明的申请操作，申请可验证声明，使得用户可以基于该可验证声明，在办理相关业务时证明自己，而无需准备相应的实体文件（如身份证），为用户提供了便利。

[89] 对应上述描述的基于区块链的可验证声明的创建方法，基于相同的技术构思，本说明书一个或多个实施例还提供一种基于区块链的可验证声明的创建方法，应用于区块链节点。图 6 为本说明书一个或多个实施例提供的一种基于区块链的可验证声明的创建方法，如图 6 所示，所述方法包括步骤 S302~S304。

[90] 步骤 S302，接收创建平台发送的可验证声明的创建记录信息，其中，创建记录信息为创建平台根据授权应用发送的创建请求，创建可验证声明之后所生成的信息。

[91] 步骤 S304，将创建记录信息保存至区块链中。

[92] 本说明书一个或多个实施例中，通过将创建记录信息保存至区块链中，能够基于

区块链的不可篡改性确保创建记录信息的真实性和有效性，从而在用户使用可验证声明办理业务时，业务提供方能够通过区块链节点基于区块链中存储的创建记录信息对用户提供的可验证声明进行验证，不仅能够确保业务安全，而且无需业务提供方对实体文件进行目检，提升了验证效率和验证的准确率。

[93] 为了便于对可验证声明的有效性进行验证，本说明书一个或多个实施例中，方法还包括：接收创建平台发送的声明处理记录信息，将声明处理记录信息保存至区块链中；其中，声明处理记录信息包括处理的可验证声明的声明标识以及表征可验证声明所处状态的有效性字段等。

[94] 基于区块链中存储的各记录信息，区块链节点可以在接收到第三方发送的声明验证请求时，对待验证的可验证声明进行全面的验证，其中，第三方可以为业务提供方，其在可验证声明验证通过时，基于可验证声明进行业务处理；例如，用户基于证明自己身份信息的可验证声明办理银行贷款业务，其中的银行即为第三方，当银行确定用户提供的可验证声明真实有效后，基于可验证声明进行用户的贷款业务的处理。具体的，方法还包括步骤 D2~D4。

[95] 步骤 D2，接收第三方发送的声明验证请求，其中，声明验证请求包括待验证的可验证声明；

[96] 步骤 D4，调用部署于区块链中的智能合约，根据区块链中存储的关于待验证的可验证声明的记录信息，对待验证的可验证声明进行验证。

[97] 由此，基于智能合约自动对待验证的可验证声明进行验证，而无需人为参与，不仅避免了人工误检的问题，提升了验证效率；而且基于区块链中存储的记录信息对可验证声明进行验证，能够确保可验证声明的真实性和有效性，从而确保业务安全。

[98] 考虑到用户可能冻结、撤销其可验证声明，因此在对待验证的可验证声明进行验证时，首先需要验证其是否处于有效状态；再者，考虑到不同的业务与用户利益的相关程度不同，例如，办理金融方面的业务与用户利益的相关性较高，如银行开户、银行贷款等；而办理入职、加入会员等业务与用户利益的相关性相对较弱。基于此，本说明书一个或多个实施例中，可以预先设定不同业务的安全等级，其中，安全等级的划分标准可以在实际应用中根据需要自行设定，例如银行开户、贷款等金融业务的安全等级高，入职、加入会员等业务的安全等级低等；或者在用户申请可验证声明时，自行设置安全机制，可验证声明中包括用户设置的安全机制信息；与之对应的，当确定基于待验证的

可验证声明所办理的业务的安全等级较低，或者根据可验证声明中的安全机制信息确定无需用户确认时，如图 7 所示，步骤 D4 中根据区块链中存储的关于待验证的可验证声明的记录信息，对待验证的可验证声明进行验证，包括步骤 E2~E6。

[99] 步骤 E2，从区块链存储的记录信息中，根据待验证的可验证声明包括的声明标识，查询关于待验证的可验证声明的目标记录信息。具体的，按照各记录信息保存至区块链的保存时间的先后顺序，根据待验证的可验证声明中的声明标识，在区块链中查询对应的最后一条记录信息，若查询到的最后一条记录信息中的有效性字段表征可验证声明处于无效状态，则将该最后一条记录信息作为目标记录信息；若查询到的最后一条记录信息中的有效性字段表征可验证声明处于有效状态，且该最后一条记录信息不是待验证的可验证声明中的声明标识所对应的唯一的记录信息，则根据待验证的可验证声明中的声明标识，在区块链中查询对应的第一条记录信息得到创建记录信息，并将创建记录信息和所述最后一条记录信息作为目标记录信息。需要指出的是，当所述最后一条记录信息是待验证的可验证声明中的声明标识所对应的唯一的记录信息时，该记录信息即为待验证的可验证声明的创建记录信息。

[100] 步骤 E4，若根据目标记录信息中的有效性字段，确定待验证的可验证声明处于有效状态，则根据目标记录信息确定待验证的可验证声明是否合法。具体的，从目标记录信息包括的所述最后一条记录信息中读取有效性字段，若读取的有效性字段表征可验证声明处于无效状态，则发送验证失败信息给第三方；若读取的有效性字段表征可验证声明处于有效状态，则根据目标记录信息中的创建记录信息确定待验证的可验证声明是否合法。

[101] 步骤 E6，若确定待验证的可验证声明合法，则确定待验证的可验证声明验证通过。

[102] 由此，在基于可验证声明所办理的业务的安全等级低，或者根据用户设置的安全机制确定无需用户确认时，基于区块链中存储的记录信息对可验证声明进行验证，确保了可验证声明的真实性和有效性，从而为业务安全提供了保障。

[103] 进一步的，为了避免可验证声明被盗用，或者在确定基于可验证声明所办理的业务的安全等级较高，或者根据用户设置的安全机制确定需要用户确认时，如图 8 所示，步骤 D4 中根据区块链中存储的创建记录信息，对待验证的可验证声明进行验证，包括：步骤 F2~F8。

[104] 步骤 F2，从区块链存储的记录信息中，根据待验证的可验证声明中的声明标识，

查询关于待验证的可验证声明的目标记录信息。本步骤的实现过程可参见前述相关描述，重复之处这里不再赘述。

[105] 步骤 F4，若根据目标记录信息中的有效性字段，确定待验证的可验证声明处于有效状态，则根据待验证的可验证声明中的用户的数字身份信息，发送业务确认请求给对应的授权应用，并确定是否通过授权应用获取到用户的确认信息。具体的，读取目标记录信息包括的所述最后一条记录信息中的有效性字段，若读取的有效性字段表征可验证声明处于无效状态，则发送验证失败信息给第三方；若读取的有效性字段表征可验证声明处于有效状态，则根据待验证的可验证声明中的用户的数字身份信息，在用户的数字身份信息与授权应用的应用标识的关联记录信息中，获取关联的应用标识；发送业务确认请求给获取的应用标识所对应的授权应用；当授权应用接收到业务确认请求时，展示业务确认请求包括的待确认信息，并在检测到用户的确认操作时，返回确认信息给区块链节点；需要指出的是，待确认信息的具体内容可以在实际应用中根据需要自行设定，本说明书实施例中对此不做具体限定。

[106] 步骤 F6，根据目标记录信息确定待验证的可验证声明是否合法。

[107] 步骤 F8，若获取到用户的确认信息且确定待验证的可验证声明合法，则确定待验证的可验证声明验证通过。

[108] 具体的，若根据目标记录信息中的有效性字段，确定待验证的可验证声明处于有效状态，则根据待验证的可验证声明中的用户的数字身份信息，发送业务确认请求给对应的授权应用，若接收到授权应用返回的确认信息，则根据目标记录信息中的创建记录信息确定待验证的可验证声明是否合法，若确定合法，则确定待验证的可验证声明验证通过。

[109] 由此，在基于可验证声明所办理的业务的安全等级较高，或者根据用户设置的安全机制确定需要用户确认时，通过发送业务确认请求给授权应用，以使用户进行确认，以及基于区块链中存储的记录信息对可验证声明进行验证，不仅能够避免可验证声明被盗用的风险，而且确保了可验证声明的真实性和有效性，为业务安全提供了保障。

[110] 需要指出的是，步骤 E2 和步骤 F2 还可以包括：从待验证的可验证声明中读取有效截止时间，若根据读取的有效截止时间确定待验证的可验证声明处于无效状态，则发送验证失败信息给第三方；若根据读取的有效截止时间确定待验证的可验证声明处于有效状态，则从区块链存储的记录信息中，根据声明标识，查询关于待验证的可验证声明

的目标记录信息。

[111] 由于不同的用户对个人信息隐私性的要求也不同，因此用户在申请可验证声明时，可以设置可验证声明的隐匿属性，当该隐匿属性为非公开时，区块链中存储的创建记录信息包括用户的数字身份信息的哈希值、创建平台的数字身份信息的哈希值、可验证声明中第二指定信息的哈希值、声明标识和有效性字段；与之对应的，步骤 E4 和步骤 F6 中，根据目标记录信息确定待验证的可验证声明是否合法，包括步骤 H2~H6。

[112] 步骤 H2，根据可验证声明中的创建平台的数字身份信息，获取创建平台的公钥，采用创建平台的公钥对可验证声明中的签名信息进行验证。具体的，根据可验证声明中的创建平台的数字身份信息索引到对应的文档（DID doc），从该文档中获取创建平台的公钥；或者，根据创建平台的数字身份信息在预先存储的创建平台的数字身份信息与公钥的关联记录信息中获取对应的公钥；或者，根据可验证声明中的创建平台的数字身份信息，发送公钥获取请求给指定平台或机构，并接收指定平台或机构发送的公钥；采用获取的公钥对可验证声明中的签名信息进行验证。

[113] 步骤 H4，计算可验证声明中的第二指定信息的哈希值，并从目标记录信息所包括的创建记录信息中，获取可验证声明对应的哈希值，将计算的第二指定信息的哈希值与获取的可验证声明对应的哈希值进行匹配。

[114] 步骤 H6，若签名信息验证通过，且哈希值匹配成功，则确定第一可验证声明合法。

[115] 具体的，根据可验证声明中的创建平台的数字身份信息，获取创建平台的公钥，采用创建平台的公钥对可验证声明中的签名信息进行验证，若验证通过，则计算可验证声明中的第二指定信息的哈希值，并从目标记录信息所包括的创建记录信息中，获取可验证声明对应的哈希值，将计算的第二指定信息的哈希值与获取的可验证声明对应的哈希值进行匹配，若匹配成功，则确定可验证声明合法。

[116] 由此，在区块链中存储有可验证声明对应的哈希值时，通过计算可验证声明中第二指定信息的哈希值，并与创建记录信息中的可验证声明对应的哈希值进行比对，实现了对可验证声明的有效性的验证，为业务安全提供了保障。

[117] 进一步的，当用户设置的可验证声明的隐匿属性为公开时，区块链中存储的创建记录信息包括可验证声明，与之对应的，步骤 E4 和步骤 F6 中，根据目标记录信息确定可验证声明是否合法，包括步骤 K2~K6。

[118] 步骤 K2，根据可验证声明中的创建平台的数字身份信息，获取创建平台的公钥，

采用创建平台的公钥对可验证声明中的签名信息进行验证。

[119] 步骤 K4，将待验证的可验证声明与创建记录信息中的可验证声明进行匹配。

[120] 步骤 K6，若匹配成功且签名信息验证通过，则确定待验证的可验证声明合法。

[121] 具体的，根据可验证声明中的创建平台的数字身份信息，获取创建平台的公钥，采用创建平台的公钥对可验证声明中的签名信息进行验证，若验证通过，则从目标记录信息包括的创建记录信息中获取可验证声明，将待验证的可验证声明与获取的可验证声明进行匹配，若匹配成功，则确定待验证的可验证声明合法。其中，获取创建平台的公钥的过程可参见前述相关描述，重复之处这里不再赘述；由此，在区块链中存储有可验证声明时，通过对待验证的可验证声明中的签名信息进行验证，以及将待验证的可验证声明与区块链中存储的可验证声明进行匹配，实现了对可验证声明的有效验证，为业务安全提供了保障。

[122] 本说明书一个或多个实施例中，通过将可验证声明的创建记录信息保存至区块链上，使得用户在基于该可验证声明办理相关业务时，能够基于区块链中存储的创建记录信息对用户提供的可验证声明进行验证，不仅能够确保业务安全，而且无需业务提供方对实体文件进行目检，提升了验证效率和验证的准确率。

[123] 对应上述图 2 至图 4 描述的基于区块链的可验证声明的创建方法，基于相同的技术构思，本说明书一个或多个实施例还提供一种基于区块链的可验证声明的创建装置，应用于创建平台。图 9 为本说明书一个或多个实施例提供的基于区块链的可验证声明的创建装置的模块组成示意图，该装置用于执行图 2 至图 4 描述的基于区块链的可验证声明的创建方法，如图 9 所示，该装置包括：接收模块 401，其接收授权应用发送的创建请求，其中，所述创建请求为所述授权应用响应于用户的可验证声明申请操作而发送，所述创建请求包括：待创建的可验证声明的声明内容和所述用户的数字身份信息；创建模块 402，其根据所述声明内容和所述数字身份信息，创建可验证声明；发送模块 403，其向所述授权应用发送所述可验证声明；生成模块 404，其生成所述可验证声明的创建记录信息，向区块链中的至少一个区块链节点发送所述创建记录信息，以使所述区块链节点将所述创建记录信息保存至区块链中。

[124] 本说明书一个或多个实施例中，通过创建可验证声明，并将创建记录信息保存至区块链上，使得用户可以基于该可验证声明，在办理相关业务时证明自己，而无需准备相应的实体文件（如身份证），为用户提供了便利；同时，对于业务提供方而言，能够

基于区块链中存储的创建记录信息对用户提供的可验证声明进行验证，不仅确保了业务安全，而且无需对实体文件进行目检，提升了验证效率和验证的准确率。

[125] 可选地，所述创建模块 402，确定创建所述可验证声明所需的字段信息；根据所述字段信息、所述声明内容、所述用户的数字身份信息及所述创建平台的数字身份信息，创建可验证声明。

[126] 可选地，所述创建模块 402，生成所述可验证声明的声明标识；以及，采用所述创建平台的私钥对预设的第一指定信息进行签名，得到签名数据；将所述声明标识和所述签名数据作为创建所述可验证声明所需的字段信息。

[127] 可选地，所述创建模块 402，确定所述创建平台是否存储有私钥；若是，则采用所述创建平台存储的私钥对预设的第一指定信息进行签名，得到签名数据；若否，则从托管平台获取与所述创建平台的私钥，并采用获取的所述私钥对预设的第一指定信息进行签名，得到签名数据。

[128] 可选地，所述生成模块 404，计算所述用户的数字身份信息的哈希值；以及，计算所述创建平台的数字身份信息的哈希值；计算所述可验证声明中第二指定信息的哈希值；将计算的各个所述哈希值、所述声明标识、有效性字段进行关联记录，并将记录的信息作为所述可验证声明的创建记录信息；其中，所述有效性字段表征所述可验证声明所处的状态。

[129] 可选地，所述生成模块 404，将所述可验证声明、所述用户的数字身份信息、所述创建平台的数字身份信息、所述声明标识和有效性字段进行关联记录，并将记录的信息作为所述可验证声明的创建记录信息；其中，所述有效性字段表征所述可验证声明所处的状态。

[130] 可选地，所述创建模块 402，将所述可验证声明、所述用户的数字身份信息、所述创建平台的数字身份信息、所述声明标识和有效性字段进行关联记录，并将记录的信息作为所述可验证声明的创建记录信息；其中，所述有效性字段表征所述可验证声明所处的状态。

[131] 可选地，所述创建模块 402 若根据所述声明内容，确定所述待创建的可验证声明所对应的安全等级满足预设条件，则向所述授权应用发送身份验证请求；以及，接收所述授权应用发送的所述用户的身份验证信息；若根据所述身份验证信息对所述用户的身份验证通过，则根据所述声明内容和所述数字身份信息，创建可验证声明。

[132] 本说明书一个或多个实施例提供的于基于区块链的可验证声明的创建装置，通过创建可验证声明，并将创建记录信息保存至区块链上，使得用户可以基于该可验证声明，在办理相关业务时证明自己，而无需准备相应的实体文件（如身份证），为用户提供了便利；同时，对于业务提供方而言，能够基于区块链中存储的创建记录信息对用户提供的可验证声明进行验证，不仅确保了业务安全，而且无需对实体文件进行目检，提升了验证效率和验证的准确率。

[133] 需要说明的是，本说明书中关于基于区块链的可验证声明的创建装置的实施例与本说明书中关于基于区块链的可验证声明的创建方法的实施例基于同一发明构思，因此该实施例的具体实施可以参见前述对应的基于区块链的可验证声明的创建方法的实施，重复之处不再赘述。

[134] 进一步地，对应上述图 5 描述的可验证声明的创建方法，基于相同的技术构思，本说明书一个或多个实施例还提供一种可验证声明的创建装置，应用于授权应用，图 10 为本说明书一个或多个实施例提供的一种可验证声明的创建装置的模块组成示意图，该装置用于执行如 5 描述的可验证声明的创建方法，如图 10 所示，该装置包括：获取模块 501，其响应于用户的可验证声明申请操作，获取待创建的可验证声明的声明内容；发送模块 502，其根据所述声明内容和所述用户的数字身份信息，向创建平台发送创建请求，以使所述创建平台根据所述声明内容和所述用户的数字身份信息，创建可验证声明；接收模块 503，其接收所述创建平台发送的所述可验证声明。

[135] 可选地，所述装置还包括：采集模块；所述接收模块 503，在所述发送模块 502 向创建平台发送创建请求之后，接收所述创建平台发送的身份验证请求；所述采集模块，采集所述用户的身份验证信息；所述发送模块 502，将所述身份验证信息发送给所述创建平台，以使所述创建平台根据所述身份验证信息对所述用户的身份进行验证。

[136] 本说明书一个或多个实施例提供的可验证声明的创建装置，响应于用户的可验证声明的申请操作，申请可验证声明，使得用户可以基于该可验证声明，在办理相关业务时证明自己，而无需准备相应的实体文件（如身份证），为用户提供了便利。

[137] 需要说明的是，本说明书中关于可验证声明的创建装置的实施例与本说明书中关于可验证声明的创建方法的实施例基于同一发明构思，因此该实施例的具体实施可以参见前述对应的可验证声明的创建方法的实施，重复之处不再赘述。

[138] 进一步地，对应上述图 6 至图 8 描述的基于区块链的可验证声明的创建方法，基

于相同的技术构思，本说明书一个或多个实施例还提供一种基于区块链的可验证声明的创建装置，应用于区块链节点；图 11 为本说明书一个或多个实施例提供的一种基于区块链的可验证声明的创建装置的模块组成示意图，该装置用于执行图 6 至图 8 描述的基于区块链的可验证声明的创建方法，如图 11 所示，该装置包括：接收模块 601，其接收创建平台发送的可验证声明的创建记录信息，其中，所述创建记录信息为所述创建平台根据授权应用发送的创建请求，创建所述可验证声明之后所生成的信息；保存模块 602，其将所述创建记录信息保存至区块链中。

[139] 本说明书一个或多个实施例中，通过将可验证声明的创建记录信息保存至区块链上，使得用户在基于该可验证声明办理相关业务时，能够基于区块链中存储的创建记录信息对用户提供的可验证声明进行验证，不仅能够确保业务安全，而且无需业务提供方对实体文件进行目检，提升了验证效率和验证的准确率。

[140] 可选地，所述装置还包括：验证模块；所述接收模块 601，接收第三方发送的声明验证请求，其中，所述声明验证请求包括待验证的可验证声明，所述第三方在所述可验证声明验证通过时，基于所述可验证声明进行业务处理；

[141] 所述验证模块，调用部署于所述区块链中的智能合约，根据所述区块链中存储的关于所述待验证的可验证声明的记录信息，对所述待验证的可验证声明进行验证。

[142] 可选地，所述待验证的可验证声明包括：声明标识和用户的数字身份信息；所述区块链中存储的关于所述待验证的可验证声明的记录信息包括：有效性字段；所述验证模块，从所述区块链存储的记录信息中，根据所述声明标识，查询关于所述待验证的可验证声明的目标记录信息；以及，若根据所述目标记录信息中的有效性字段，确定所述待验证的可验证声明处于有效状态，则根据所述用户的数字身份信息，发送业务确认请求给所述授权应用，并确定是否通过所述授权应用获取到所述用户的确认信息；以及，根据所述目标记录信息确定所述待验证的可验证声明是否合法；若获取到所述用户的确认信息且确定所述待验证的可验证声明合法，则确定所述待验证的可验证声明验证通过。

[143] 可选地，所述待验证的可验证声明包括：声明标识；所述区块链中存储的关于所述待验证的可验证声明的记录信息包括：有效性字段；所述验证模块，从所述区块链存储的记录信息中，根据所述声明标识，查询关于所述待验证的可验证声明的目标记录信息；若根据所述目标记录信息中的有效性字段，确定所述待验证的可验证声明处于有效状态，则根据所述目标记录信息确定所述待验证的可验证声明是否合法；若确定所述待验证的可验证声明合法，则确定所述待验证的可验证声明验证通过。

[144] 可选地，所述待验证的可验证声明包括：签名信息，所述目标记录信息包括：创建记录信息；所述验证模块，根据所述待验证的可验证声明包括的创建平台的数字身份信息，获取所述创建平台的公钥，采用所述创建平台的公钥对所述签名信息进行验证；以及，计算所述待验证的可验证声明中的第二指定信息的哈希值，并获取所述创建记录信息中的所述可验证声明对应的哈希值，将计算的所述第二指定信息的哈希值与所述可验证声明对应的哈希值进行匹配；若所述签名信息验证通过，且所述哈希值匹配成功，则确定所述待验证的可验证声明合法。

[145] 可选地，所述第一可验证声明包括：签名信息；所述目标记录信息包括：创建记录信息；所述验证模块，根据所述待验证的可验证声明包括的创建平台的数字身份信息，获取所述创建平台的公钥，采用所述创建平台的公钥对所述签名信息进行验证；以及，将所述待验证的可验证声明与所述创建记录信息中的可验证声明进行匹配；若匹配成功且所述签名信息验证通过，则确定所述待验证的可验证声明合法。

[146] 本说明书一个或多个实施例提供的基于区块链的可验证声明的创建装置，通过将可验证声明的创建记录信息保存至区块链上，使得用户在基于该可验证声明办理相关业务时，能够基于区块链中存储的创建记录信息对用户提供的可验证声明进行验证，不仅能够确保业务安全，而且无需业务提供方对实体文件进行目检，提升了验证效率和验证的准确率。

[147] 需要说明的是，本说明书中关于基于区块链的可验证声明的创建装置的实施例与本说明书中关于基于区块链的可验证声明的创建方法的实施例基于同一发明构思，因此该实施例的具体实施可以参见前述对应的基于区块链的可验证声明的创建方法的实施，重复之处不再赘述。

[148] 进一步地，对应上述描述的方法，基于相同的技术构思，本说明书一个或多个实施例还提供一种基于区块链的可验证声明的创建系统，图 12 为本说明书一个或多个实施例提供的一种基于区块链的可验证声明的创建系统的组成示意图，如图 12 所示，该系统包括：授权应用 701、创建平台 702 和区块链 703。

[149] 所述授权应用 701，响应于用户的可验证声明申请操作，获取待创建的可验证声明的声明内容，根据所述声明内容和所述用户的数字身份信息，向所述创建平台 702 发送创建请求。

[150] 所述创建平台 702，根据所述声明内容和所述数字身份信息，创建可验证声明，向

所述授权应用 701 发送所述可验证声明；以及，生成所述可验证声明的创建记录信息，将所述创建记录信息发送给所述区块链 703 中的至少一个区块链节点。

[151] 所述区块链 703 中的区块链节点，在接收到所述创建记录信息时，将所述创建记录信息保存至区块链中。

[152] 本说明书一个或多个实施例提供的基于区块链的可验证声明的创建系统，通过创建可验证声明，并将创建记录信息保存至区块链上，使得用户可以基于该可验证声明，在办理相关业务时证明自己，而无需准备相应的实体文件（如身份证），为用户提供了便利；同时，对于业务提供方而言，能够基于区块链中存储的创建记录信息对用户提供的可验证声明进行验证，不仅确保了业务安全，而且无需对实体文件进行目检，提升了验证效率和验证的准确率。

[153] 需要说明的是，本说明书中关于基于区块链的可验证声明的创建系统的实施例与本说明书中关于基于区块链的可验证声明的创建方法的实施例基于同一发明构思，因此该实施例的具体实施可以参见前述对应的基于区块链的可验证声明的创建方法的实施，重复之处不再赘述。

[154] 进一步地，对应上述描述的基于区块链的可验证声明的创建方法，基于相同的技术构思，本说明书一个或多个实施例还提供一种基于区块链的可验证声明的创建设备，该设备用于执行上述的基于区块链的可验证声明的创建方法，图 13 为本说明书一个或多个实施例提供的一种基于区块链的可验证声明的创建设备的结构示意图。

[155] 如图 13 所示，基于区块链的可验证声明的创建设备可因配置或性能不同而产生比较大的差异，可以包括一个或一个以上的处理器 801 和存储器 802，存储器 802 中可以存储有一个或一个以上存储应用程序或数据。其中，存储器 802 可以是短暂存储或持久存储。存储在存储器 802 的应用程序可以包括一个或一个以上模块（图示未示出），每个模块可以包括基于区块链的可验证声明的创建设备中的一系列计算机可执行指令。更进一步地，处理器 801 可以设置为与存储器 802 通信，在基于区块链的可验证声明的创建设备上执行存储器 802 中的一系列计算机可执行指令。基于区块链的可验证声明的创建设备还可以包括一个或一个以上电源 803，一个或一个以上有线或无线网络接口 804，一个或一个以上输入输出接口 805，一个或一个以上键盘 806 等。

[156] 在一个具体的实施例中，基于区块链的可验证声明的创建设备包括有存储器，以及一个或一个以上的程序，其中一个或者一个以上程序存储于存储器中，且一个或者一

个以上程序可以包括一个或一个以上模块，且每个模块可以包括对基于区块链的可验证声明的创建设备中的一系列计算机可执行指令，且经配置以由一个或者一个以上处理器执行该一个或者一个以上程序包含用于进行以下计算机可执行指令：接收授权应用发送的创建请求，其中，所述创建请求为所述授权应用响应于用户的可验证声明申请操作而发送，所述创建请求包括：待创建的可验证声明的声明内容和所述用户的数字身份信息；根据所述声明内容和所述数字身份信息，创建可验证声明；向所述授权应用发送所述可验证声明；生成所述可验证声明的创建记录信息，向区块链中的至少一个区块链节点发送所述创建记录信息，以使所述区块链节点将所述创建记录信息保存至区块链中。

[157] 本说明书一个或多个实施例中，通过创建可验证声明，并将创建记录信息保存至区块链上，使得用户可以基于该可验证声明，在办理相关业务时证明自己，而无需准备相应的实体文件（如身份证），为用户提供了便利；同时，对于业务提供方而言，能够基于区块链中存储的创建记录信息对用户提供的可验证声明进行验证，不仅确保了业务安全，而且无需对实体文件进行目检，提升了验证效率和验证的准确率。

[158] 可选地，计算机可执行指令在被执行时，根据所述声明内容和所述数字身份信息，创建可验证声明，包括：确定创建所述可验证声明所需的字段信息；根据所述字段信息、所述声明内容、所述用户的数字身份信息及所述创建平台的数字身份信息，创建可验证声明。

[159] 可选地，计算机可执行指令在被执行时，所述确定创建所述可验证声明所需的字段信息，包括：生成所述可验证声明的声明标识；采用所述创建平台的私钥对预设的第一指定信息进行签名，得到签名数据；将所述声明标识和所述签名数据作为创建所述可验证声明所需的字段信息。

[160] 可选地，计算机可执行指令在被执行时，所述采用创建平台的私钥对预设的第一指定信息进行签名，得到签名数据，包括：确定所述创建平台是否存储有私钥；若是，则采用所述创建平台存储的私钥对预设的第一指定信息进行签名，得到签名数据；若否，则从托管平台获取与所述创建平台的私钥，并采用获取的所述私钥对预设的第一指定信息进行签名，得到签名数据。

[161] 可选地，计算机可执行指令在被执行时，所述生成所述可验证声明的创建记录信息，包括：计算所述用户的数字身份信息的哈希值；计算所述创建平台的数字身份信息的哈希值；计算所述可验证声明中第二指定信息的哈希值；将计算的各个所述哈希值、所述声明标识、有效性字段进行关联记录，并将记录的信息作为所述可验证声明的创建

记录信息；其中，所述有效性字段表征所述可验证声明所处的状态。

[162] 可选地，计算机可执行指令在被执行时，所述生成所述可验证声明的创建记录信息，包括：将所述可验证声明、所述用户的数字身份信息、所述创建平台的数字身份信息、所述声明标识和有效性字段进行关联记录，并将记录的信息作为所述可验证声明的创建记录信息；其中，所述有效性字段表征所述可验证声明所处的状态。

[163] 可选地，计算机可执行指令在被执行时，根据所述声明内容和所述数字身份信息，创建可验证声明，包括：若根据所述声明内容，确定所述待创建的可验证声明所对应的安全等级满足预设条件，则向所述授权应用发送身份验证请求；接收所述授权应用发送的所述用户的身份验证信息；若根据所述身份验证信息对所述用户的身份验证通过，则根据所述声明内容和所述数字身份信息，创建可验证声明。

[164] 本说明书一个或多个实施例提供的基于区块链的可验证声明的创建设备，通过创建可验证声明，并将创建记录信息保存至区块链上，使得用户可以基于该可验证声明，在办理相关业务时证明自己，而无需准备相应的实体文件（如身份证），为用户提供了便利；同时，对于业务提供方而言，能够基于区块链中存储的创建记录信息对用户提供的可验证声明进行验证，不仅确保了业务安全，而且无需对实体文件进行目检，提升了验证效率和验证的准确率。

[165] 在另一个具体的实施例中，基于区块链的可验证声明的创建设备包括有存储器，以及一个或一个以上的程序，其中一个或者一个以上程序存储于存储器中，且一个或者一个以上程序可以包括一个或一个以上模块，且每个模块可以包括对基于区块链的可验证声明的创建设备中的一系列计算机可执行指令，且经配置以由一个或者一个以上处理器执行该一个或者一个以上程序包含用于进行以下计算机可执行指令：

[166] 接收创建平台发送的可验证声明的创建记录信息，其中，所述创建记录信息为所述创建平台根据授权应用发送的创建请求，创建所述可验证声明之后所生成的信息；将所述创建记录信息保存至区块链中。

[167] 本说明书一个或多个实施例中，通过将创建记录信息保存至区块链中，能够基于区块链的不可篡改性确保创建记录信息的真实性和有效性，从而在用户使用可验证声明办理业务时，业务提供方能够通过区块链节点基于区块链中存储的创建记录信息对用户提供的可验证声明进行验证，不仅能够确保业务安全，而且无需业务提供方对实体文件进行目检，提升了验证效率和验证的准确率。

[168] 可选地，计算机可执行指令在被执行时，所述方法还包括：接收第三方发送的声明验证请求，其中，所述声明验证请求包括待验证的可验证声明，所述第三方在所述可验证声明验证通过时，基于所述可验证声明进行业务处理；调用部署于所述区块链中的智能合约，根据所述区块链中存储的关于所述待验证的可验证声明的记录信息，对所述待验证的可验证声明进行验证。

[169] 可选地，计算机可执行指令在被执行时，所述待验证的可验证声明包括：声明标识和用户的数字身份信息；所述区块链中存储的关于所述待验证的可验证声明的记录信息包括：有效性字段；根据所述区块链中存储的关于所述待验证的可验证声明的记录信息，对所述待验证的可验证声明进行验证，包括：从所述区块链存储的记录信息中，根据所述声明标识，查询关于所述待验证的可验证声明的目标记录信息；若根据所述目标记录信息中的有效性字段，确定所述待验证的可验证声明处于有效状态，则根据所述用户的数字身份信息，发送业务确认请求给所述授权应用，并确定是否通过所述授权应用获取到所述用户的确认信息；以及，根据所述目标记录信息确定所述待验证的可验证声明是否合法；若获取到所述用户的确认信息且确定所述待验证的可验证声明合法，则确定所述待验证的可验证声明验证通过。

[170] 可选地，计算机可执行指令在被执行时，所述待验证的可验证声明包括：声明标识；所述区块链中存储的关于所述待验证的可验证声明的记录信息包括：有效性字段；根据所述区块链中存储的关于所述待验证的可验证声明的记录信息，对所述待验证的可验证声明进行验证，包括：从所述区块链存储的记录信息中，根据所述声明标识，查询关于所述待验证的可验证声明的目标记录信息；若根据所述目标记录信息中的有效性字段，确定所述待验证的可验证声明处于有效状态，则根据所述目标记录信息确定所述待验证的可验证声明是否合法；若确定所述待验证的可验证声明合法，则确定所述待验证的可验证声明验证通过。

[171] 可选地，计算机可执行指令在被执行时，所述待验证的可验证声明包括：签名信息；所述目标记录信息包括：创建记录信息；根据所述目标记录信息确定所述待验证的可验证声明是否合法，包括：根据所述待验证的可验证声明包括的创建平台的数字身份信息，获取所述创建平台的公钥，采用所述创建平台的公钥对所述签名信息进行验证；以及，计算所述待验证的可验证声明中的第二指定信息的哈希值，并获取所述创建记录信息中的所述可验证声明对应的哈希值，将计算的所述第二指定信息的哈希值与所述可验证声明对应的哈希值进行匹配；若所述签名信息验证通过，且所述哈希值匹配成功，

则确定所述待验证的可验证声明合法。

[172] 可选地，计算机可执行指令在被执行时，所述第一可验证声明包括：签名信息；所述目标记录信息包括：创建记录信息；根据所述目标记录信息确定所述待验证的可验证声明是否合法，包括：根据所述待验证的可验证声明包括的创建平台的数字身份信息，获取所述创建平台的公钥，采用所述创建平台的公钥对所述签名信息进行验证；以及，将所述待验证的可验证声明与所述创建记录信息中的可验证声明进行匹配；若匹配成功且所述签名信息验证通过，则确定所述待验证的可验证声明合法。

[173] 本说明书一个或多个实施例提供的基于区块链的可验证声明的创建设备，通过将创建记录信息保存至区块链中，能够基于区块链的不可篡改性确保创建记录信息的真实性和有效性，从而在用户使用可验证声明办理业务时，业务提供方能够通过区块链节点基于区块链中存储的创建记录信息对用户提供的可验证声明进行验证，不仅能够确保业务安全，而且无需业务提供方对实体文件进行目检，提升了验证效率和验证的准确率。

[174] 需要说明的是，本说明书中关于基于区块链的可验证声明的创建设备的实施例与本说明书中关于基于区块链的可验证声明的创建方法的实施例基于同一发明构思，因此该实施例的具体实施可以参见前述对应的基于区块链的可验证声明的创建方法的实施，重复之处不再赘述。

[175] 进一步地，对应上述描述的可验证声明的创建方法，基于相同的技术构思，本说明书一个或多个实施例还提供一种可验证声明的创建设备，该设备用于执行上述的可验证声明的创建方法，图 14 为本说明书一个或多个实施例提供的一种可验证声明的创建设备的结构示意图。

[176] 如图 14 所示，可验证声明的创建设备可因配置或性能不同而产生比较大的差异，可以包括一个或一个以上的处理器 901 和存储器 902，存储器 902 中可以存储有一个或一个以上存储应用程序或数据。其中，存储器 902 可以是短暂存储或持久存储。存储在存储器 902 的应用程序可以包括一个或一个以上模块（图示未示出），每个模块可以包括可验证声明的创建设备中的一系列计算机可执行指令。更进一步地，处理器 901 可以设置为与存储器 902 通信，在可验证声明的创建设备上执行存储器 902 中的一系列计算机可执行指令。可验证声明的创建设备还可以包括一个或一个以上电源 903，一个或一个以上有线或无线网络接口 904，一个或一个以上输入输出接口 905，一个或一个以上键盘 906 等。

[177] 在一个具体的实施例中，可验证声明的创建设备包括有存储器，以及一个或一个以上的程序，其中一个或者一个以上程序存储于存储器中，且一个或者一个以上程序可以包括一个或一个以上模块，且每个模块可以包括对可验证声明的创建设备中的一系列计算机可执行指令，且经配置以由一个或者一个以上处理器执行该一个或者一个以上程序包含用于进行以下计算机可执行指令：响应于用户的可验证声明申请操作，获取待创建的可验证声明的声明内容；根据所述声明内容和所述用户的数字身份信息，向创建平台发送创建请求，以使所述创建平台根据所述声明内容和所述用户的数字身份信息，创建可验证声明；接收所述创建平台发送的所述可验证声明。

[178] 可选地，计算机可执行指令在被执行时，所述向创建平台发送创建请求之后，还包括：接收所述创建平台发送的身份验证请求；采集所述用户的身份验证信息；将所述身份验证信息发送给所述创建平台，以使所述创建平台根据所述身份验证信息对所述用户的身份进行认证。

[179] 本说明书一个或多个实施例提供的可验证声明的创建设备，响应于用户的可验证声明的申请操作，申请可验证声明，使得用户可以基于该可验证声明，在办理相关业务时证明自己，而无需准备相应的实体文件（如身份证），为用户提供了便利。

[180] 需要说明的是，本说明书中关于可验证声明的创建设备的实施例与本说明书中关于可验证声明的创建方法的实施例基于同一发明构思，因此该实施例的具体实施可以参见前述对应的可验证声明的创建方法的实施，重复之处不再赘述。

[181] 进一步地，对应上述描述的方法，基于相同的技术构思，本说明书一个或多个实施例还提供了一种存储介质，用于存储计算机可执行指令，一个具体的实施例中，该存储介质可以为 U 盘、光盘、硬盘等，该存储介质存储的计算机可执行指令在被处理器执行时，能实现以下流程：接收授权应用发送的创建请求，其中，所述创建请求为所述授权应用响应于用户的可验证声明申请操作而发送，所述创建请求包括：待创建的可验证声明的声明内容和所述用户的数字身份信息；根据所述声明内容和所述数字身份信息，创建可验证声明；向所述授权应用发送所述可验证声明；生成所述可验证声明的创建记录信息，向区块链中的至少一个区块链节点发送所述创建记录信息，以使所述区块链节点将所述创建记录信息保存至区块链中。

[182] 本说明书一个或多个实施例中，通过创建可验证声明，并将创建记录信息保存至区块链上，使得用户可以基于该可验证声明，在办理相关业务时证明自己，而无需准备相应的实体文件（如身份证），为用户提供了便利；同时，对于业务提供方而言，能够

基于区块链中存储的创建记录信息对用户提供的可验证声明进行验证，不仅确保了业务安全，而且无需对实体文件进行目检，提升了验证效率和验证的准确率。

[183] 可选地，该存储介质存储的计算机可执行指令在被处理器执行时，根据所述声明内容和所述数字身份信息，创建可验证声明，包括：确定创建所述可验证声明所需的字段信息；根据所述字段信息、所述声明内容、所述用户的数字身份信息及所述创建平台的数字身份信息，创建可验证声明。

[184] 可选地，该存储介质存储的计算机可执行指令在被处理器执行时，所述确定创建所述可验证声明所需的字段信息，包括：生成所述可验证声明的声明标识；采用所述创建平台的私钥对预设的第一指定信息进行签名，得到签名数据；将所述声明标识和所述签名数据作为创建所述可验证声明所需的字段信息。

[185] 可选地，该存储介质存储的计算机可执行指令在被处理器执行时，所述采用创建平台的私钥对预设的第一指定信息进行签名，得到签名数据，包括：确定所述创建平台是否存储有私钥；若是，则采用所述创建平台存储的私钥对预设的第一指定信息进行签名，得到签名数据；若否，则从托管平台获取与所述创建平台的私钥，并采用获取的所述私钥对预设的第一指定信息进行签名，得到签名数据。

[186] 可选地，该存储介质存储的计算机可执行指令在被处理器执行时，所述生成所述可验证声明的创建记录信息，包括：计算所述用户的数字身份信息的哈希值；计算所述创建平台的数字身份信息的哈希值；计算所述可验证声明中第二指定信息的哈希值；将计算的各个所述哈希值、所述声明标识、有效性字段进行关联记录，并将记录的信息作为所述可验证声明的创建记录信息；其中，所述有效性字段表征所述可验证声明所处的状态。

[187] 可选地，该存储介质存储的计算机可执行指令在被处理器执行时，所述生成所述可验证声明的创建记录信息，包括：将所述可验证声明、所述用户的数字身份信息、所述创建平台的数字身份信息、所述声明标识和有效性字段进行关联记录，并将记录的信息作为所述可验证声明的创建记录信息；其中，所述有效性字段表征所述可验证声明所处的状态。

[188] 可选地，该存储介质存储的计算机可执行指令在被处理器执行时，根据所述声明内容和所述数字身份信息，创建可验证声明，包括：若根据所述声明内容，确定所述待创建的可验证声明所对应的安全等级满足预设条件，则向所述授权应用发送身份验证请

求；接收所述授权应用发送的所述用户的身份验证信息；若根据所述身份验证信息对所述用户的身份验证通过，则根据所述声明内容和所述数字身份信息，创建可验证声明。

[189] 本说明书一个或多个实施例提供的存储介质存储的计算机可执行指令在被处理器执行时，通过创建可验证声明，并将创建记录信息保存至区块链上，使得用户可以基于该可验证声明，在办理相关业务时证明自己，而无需准备相应的实体文件（如身份证），为用户提供了便利；同时，对于业务提供方而言，能够基于区块链中存储的创建记录信息对用户提供的可验证声明进行验证，不仅确保了业务安全，而且无需对实体文件进行目检，提升了验证效率和验证的准确率。

[190] 另一个具体的实施例中，该存储介质可以为 U 盘、光盘、硬盘等，该存储介质存储的计算机可执行指令在被处理器执行时，能实现以下流程：响应于用户的可验证声明申请操作，获取待创建的可验证声明的声明内容；根据所述声明内容和所述用户的数字身份信息，向创建平台发送创建请求，以使所述创建平台根据所述声明内容和所述用户的数字身份信息，创建可验证声明；接收所述创建平台发送的所述可验证声明。

[191] 可选地，该存储介质存储的计算机可执行指令在被处理器执行时，接收所述创建平台发送的身份验证请求；采集所述用户的身份验证信息；将所述身份验证信息发送给所述创建平台，以使所述创建平台根据所述身份验证信息对所述用户的身份进行认证。

[192] 本说明书一个或多个实施例提供的存储介质存储的计算机可执行指令在被处理器执行时，响应于用户的可验证声明的申请操作，申请可验证声明，使得用户可以基于该可验证声明，在办理相关业务时证明自己，而无需准备相应的实体文件（如身份证），为用户提供了便利。

[193] 另一个具体的实施例中，该存储介质可以为 U 盘、光盘、硬盘等，该存储介质存储的计算机可执行指令在被处理器执行时，能实现以下流程：接收创建平台发送的可验证声明的创建记录信息，其中，所述创建记录信息为所述创建平台根据授权应用发送的创建请求，创建所述可验证声明之后所生成的信息；将所述创建记录信息保存至区块链中。

[194] 本说明书一个或多个实施例中，通过将创建记录信息保存至区块链中，能够基于区块链的不可篡改性确保创建记录信息的真实性和有效性，从而在用户使用可验证声明办理业务时，业务提供方能够通过区块链节点基于区块链中存储的创建记录信息对用户提供的可验证声明进行验证，不仅能够确保业务安全，而且无需业务提供方对实体文件

进行目检，提升了验证效率和验证的准确率。

[195] 可选地，该存储介质存储的计算机可执行指令在被处理器执行时，所述方法还包括：接收第三方发送的声明验证请求，其中，所述声明验证请求包括待验证的可验证声明，所述第三方在所述可验证声明验证通过时，基于所述可验证声明进行业务处理；调用部署于所述区块链中的智能合约，根据所述区块链中存储的关于所述待验证的可验证声明的记录信息，对所述待验证的可验证声明进行验证。

[196] 可选地，该存储介质存储的计算机可执行指令在被处理器执行时，所述待验证的可验证声明包括：声明标识和用户的数字身份信息；所述区块链中存储的关于所述待验证的可验证声明的记录信息包括：有效性字段；根据所述区块链中存储的关于所述待验证的可验证声明的记录信息，对所述待验证的可验证声明进行验证，包括：从所述区块链存储的记录信息中，根据所述声明标识，查询关于所述待验证的可验证声明的目标记录信息；若根据所述目标记录信息中的有效性字段，确定所述待验证的可验证声明处于有效状态，则根据所述用户的数字身份信息，发送业务确认请求给所述授权应用，并确定是否通过所述授权应用获取到所述用户的确认信息；以及，根据所述目标记录信息确定所述待验证的可验证声明是否合法；若获取到所述用户的确认信息且确定所述待验证的可验证声明合法，则确定所述待验证的可验证声明验证通过。

[197] 可选地，该存储介质存储的计算机可执行指令在被处理器执行时，所述待验证的可验证声明包括：声明标识；所述区块链中存储的关于所述待验证的可验证声明的记录信息包括：有效性字段；根据所述区块链中存储的关于所述待验证的可验证声明的记录信息，对所述待验证的可验证声明进行验证，包括：从所述区块链存储的记录信息中，根据所述声明标识，查询关于所述待验证的可验证声明的目标记录信息；若根据所述目标记录信息中的有效性字段，确定所述待验证的可验证声明处于有效状态，则根据所述目标记录信息确定所述待验证的可验证声明是否合法；若确定所述待验证的可验证声明合法，则确定所述待验证的可验证声明验证通过。

[198] 可选地，该存储介质存储的计算机可执行指令在被处理器执行时，所述待验证的可验证声明包括：签名信息；所述目标记录信息包括：创建记录信息；根据所述目标记录信息确定所述待验证的可验证声明是否合法，包括：根据所述待验证的可验证声明包括的创建平台的数字身份信息，获取所述创建平台的公钥，采用所述创建平台的公钥对所述签名信息进行验证；以及，计算所述待验证的可验证声明中的第二指定信息的哈希值，并获取所述创建记录信息中的所述可验证声明对应的哈希值，将计算的所述第二指

定信息的哈希值与所述可验证声明对应的哈希值进行匹配；若所述签名信息验证通过，且所述哈希值匹配成功，则确定所述待验证的可验证声明合法。

[199] 可选地，该存储介质存储的计算机可执行指令在被处理器执行时，所述待验证的可验证声明包括：签名信息；所述目标记录信息包括：创建记录信息；根据所述目标记录信息确定所述待验证的可验证声明是否合法，包括：根据所述待验证的可验证声明包括的创建平台的数字身份信息，获取所述创建平台的公钥，采用所述创建平台的公钥对所述签名信息进行验证；以及，将所述待验证的可验证声明与所述创建记录信息中的可验证声明进行匹配；若匹配成功且所述签名信息验证通过，则确定所述待验证的可验证声明合法。

[200] 本说明书一个或多个实施例提供的存储介质存储的计算机可执行指令在被处理器执行时，通过将创建记录信息保存至区块链中，能够基于区块链的不可篡改性确保创建记录信息的真实性和有效性，从而在用户使用可验证声明办理业务时，业务提供方能够通过区块链节点基于区块链中存储的创建记录信息对用户提供的可验证声明进行验证，不仅能够确保业务安全，而且无需业务提供方对实体文件进行目检，提升了验证效率和验证的准确率。

[201] 需要说明的是，本说明书中关于存储介质的实施例与本说明书中关于基于区块链的可验证声明的创建方法、或者可验证声明的创建方法的实施例基于同一发明构思，因此该实施例的具体实施可以参见前述对应方法的实施，重复之处不再赘述。

[202] 上述对本说明书特定实施例进行了描述。其它实施例在所附权利要求书的范围内。在一些情况下，在权利要求书中记载的动作或步骤可以按照不同于实施例中的顺序来执行并且仍然可以实现期望的结果。另外，在附图中描绘的过程不一定要求示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中，多任务处理和并行处理也是可以的或者可能是有利的。

[203] 在 20 世纪 30 年代，对于一个技术的改进可以很明显地区分是硬件上的改进（例如，对二极管、晶体管、开关等电路结构的改进）还是软件上的改进（对于方法流程的改进）。然而，随着技术的发展，当今的很多方法流程的改进已经可以视为硬件电路结构的直接改进。设计人员几乎都通过将改进的方法流程编程到硬件电路中来得到相应的硬件电路结构。因此，不能说一个方法流程的改进就不能用硬件实体模块来实现。例如，可编程逻辑器件（Programmable Logic Device，PLD）（例如现场可编程门阵列（Field Programmable Gate Array，FPGA））就是这样一种集成电路，其逻辑功能由用户对器件

编程来确定。由设计人员自行编程来把一个数字系统“集成”在一片 PLD 上，而不需要请芯片制造厂商来设计和制作专用的集成电路芯片。而且，如今，取代手工地制作集成电路芯片，这种编程也多半改用“逻辑编译器（logic compiler）”软件来实现，它与程序开发撰写时所用的软件编译器相类似，而要编译之前的原始代码也得用特定的编程语言来撰写，此称之为硬件描述语言（Hardware Description Language，HDL），而 HDL 也并非仅有一种，而是有许多种，如 ABEL（Advanced Boolean Expression Language）、AHDL（Altera Hardware Description Language）、Confluence、CUPL（Cornell University Programming Language）、HDCal、JHDL（Java Hardware Description Language）、Lava、Lola、MyHDL、PALASM、RHDL（Ruby Hardware Description Language）等，目前最普遍使用的是 VHDL（Very-High-Speed Integrated Circuit Hardware Description Language）与 Verilog。本领域技术人员也应该清楚，只需要将方法流程用上述几种硬件描述语言稍作逻辑编程并编程到集成电路中，就可以很容易得到实现该逻辑方法流程的硬件电路。

[204] 控制器可以按任何适当的方式实现，例如，控制器可以采取例如微处理器或处理器以及存储可由该（微）处理器执行的计算机可读程序代码（例如软件或固件）的计算机可读介质、逻辑门、开关、专用集成电路（Application Specific Integrated Circuit，ASIC）、可编程逻辑控制器和嵌入微控制器的形式，控制器的例子包括但不限于以下微控制器：ARC 625D、Atmel AT91SAM、Microchip PIC18F26K20 以及 Silicone Labs C9051F320，存储器控制器还可以被实现为存储器的控制逻辑的一部分。本领域技术人员也知道，除了以纯计算机可读程序代码方式实现控制器以外，完全可以通过将方法步骤进行逻辑编程来使得控制器以逻辑门、开关、专用集成电路、可编程逻辑控制器和嵌入微控制器等的形式来实现相同功能。因此这种控制器可以被认为是一种硬件部件，而对其内包括的用于实现各种功能的装置也可以视为硬件部件内的结构。或者甚至，可以将用于实现各种功能的装置视为既可以是实现方法的软件模块又可以是硬件部件内的结构。

[205] 上述实施例阐明的系统、装置、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。具体的，计算机例如可以为个人计算机、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何设备的组合。

[206] 为了描述的方便，描述以上装置时以功能分为各种单元分别描述。当然，在实施本说明书实施例时可以把各单元的功能在同一个或多个软件和/或硬件中实现。

[207] 本领域内的技术人员应明白，本说明书一个或多个实施例可提供为方法、系统或计算机程序产品。因此，本说明书一个或多个实施例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，本说明书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。

[208] 本说明书是参照根据本说明书实施例的方法、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。

[209] 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。

[210] 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。

[211] 在一个典型的配置中，计算设备包括一个或多个处理器（CPU）、输入/输出接口、网络接口和内存。

[212] 内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器（RAM）和/或非易失性内存等形式，如只读存储器（ROM）或闪存（flash RAM）。内存是计算机可读介质的示例。

[213] 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。

[214] 还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

[215] 本说明书一个或多个实施例可以在由计算机执行的计算机可执行指令的一般上下文中描述，例如程序模块。一般地，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等等。也可以在分布式计算环境中实践本说明书的一个或多个实施例，在这些分布式计算环境中，由通过通信网络而被连接的远程处理设备来执行任务。在分布式计算环境中，程序模块可以位于包括存储设备在内的本地和远程计算机存储介质中。

[216] 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，对于系统实施例而言，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。

[217] 以上所述仅为本文件的实施例而已，并不用于限制本文件。对于本领域技术人员来说，本文件可以有各种更改和变化。凡在本文件的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在本文件的权利要求范围之内。

权利要求书

1、一种基于区块链的可验证声明的创建方法，应用于可验证声明的创建平台，包括:

接收授权应用发送的创建请求，其中，所述创建请求为所述授权应用响应于用户的可验证声明申请操作而发送，所述创建请求包括：待创建的可验证声明的声明内容和所述用户的数字身份信息;

根据所述声明内容和所述数字身份信息，创建可验证声明;

向所述授权应用发送所述可验证声明;

生成所述可验证声明的创建记录信息，向区块链中的至少一个区块链节点发送所述创建记录信息，以使所述区块链节点将所述创建记录信息保存至区块链中。

2、根据权利要求 1 所述的方法，根据所述声明内容和所述数字身份信息，创建可验证声明，包括:

确定创建所述可验证声明所需的字段信息;

根据所述字段信息、所述声明内容、所述用户的数字身份信息及所述创建平台的数字身份信息，创建可验证声明。

3、根据权利要求 2 所述的方法，所述确定创建所述可验证声明所需的字段信息，包括:

生成所述可验证声明的声明标识;

采用所述创建平台的私钥对预设的第一指定信息进行签名，得到签名数据;

将所述声明标识和所述签名数据作为创建所述可验证声明所需的字段信息。

4、根据权利要求 3 所述的方法，所述采用所述创建平台的私钥对预设的第一指定信息进行签名，得到签名数据，包括:

确定所述创建平台是否存储有私钥;

若是，则采用所述创建平台存储的私钥对预设的第一指定信息进行签名，得到签名数据;

若否，则从托管平台获取所述创建平台的私钥，并采用获取的所述私钥对预设的第一指定信息进行签名，得到签名数据。

5、根据权利要求 3 所述的方法，生成所述可验证声明的创建记录信息，包括:

计算所述用户的数字身份信息的哈希值;

计算所述创建平台的数字身份信息的哈希值;

计算所述可验证声明中第二指定信息的哈希值;

将计算的各个所述哈希值、所述声明标识、有效性字段进行关联记录，并将记录的信息作为所述可验证声明的创建记录信息；其中，所述有效性字段表征所述可验证声明所处的状态。

6、根据权利要求 3 所述的方法，生成所述可验证声明的创建记录信息，包括：

将所述可验证声明、所述用户的数字身份信息、所述创建平台的数字身份信息、所述声明标识和有效性字段进行关联记录，并将记录的信息作为所述可验证声明的创建记录信息；其中，所述有效性字段表征所述可验证声明所处的状态。

7、根据权利要求 1-6 中任一项所述的方法，根据所述声明内容和所述数字身份信息，创建可验证声明，包括：

若根据所述声明内容，确定所述待创建的可验证声明所对应的安全等级满足预设条件，则向所述授权应用发送身份验证请求；

接收所述授权应用发送的所述用户的身份验证信息；

若根据所述身份验证信息对所述用户的身份验证通过，则根据所述声明内容和所述数字身份信息，创建可验证声明。

8、一种可验证声明的创建方法，应用于授权应用，包括：

响应于用户的可验证声明申请操作，获取待创建的可验证声明的声明内容；

根据所述声明内容和所述用户的数字身份信息，向创建平台发送创建请求，以使所述创建平台根据所述声明内容和所述用户的数字身份信息，创建可验证声明；

接收所述创建平台发送的所述可验证声明。

9、根据权利要求 8 所述的方法，所述可验证声明所对应的安全等级满足预设条件，所述向创建平台发送创建请求之后，还包括：

接收所述创建平台发送的身份验证请求；

采集所述用户的身份验证信息；

将所述身份验证信息发送给所述创建平台，以使所述创建平台根据所述身份验证信息对所述用户的身份进行验证。

10、一种基于区块链的可验证声明的创建方法，应用于区块链中的区块链节点，包括：

接收创建平台发送的可验证声明的创建记录信息，其中，所述创建记录信息为所述创建平台根据授权应用发送的创建请求，创建所述可验证声明之后所生成的信息；

将所述创建记录信息保存至区块链中。

11、根据权利要求 10 所述的方法，所述方法还包括：

接收第三方发送的声明验证请求，其中，所述声明验证请求包括待验证的可验证声明，所述第三方在所述可验证声明验证通过时，基于所述可验证声明进行业务处理；

调用部署于所述区块链中的智能合约，根据所述区块链中存储的关于所述待验证的可验证声明的记录信息，对所述待验证的可验证声明进行验证。

12、根据权利要求 11 所述的方法，所述待验证的可验证声明包括：声明标识和用户的数字身份信息；所述区块链中存储的关于所述待验证的可验证声明的记录信息包括：有效性字段；

根据所述区块链中存储的关于所述待验证的可验证声明的记录信息，对所述待验证的可验证声明进行验证，包括：

从所述区块链存储的记录信息中，根据所述声明标识，查询关于所述待验证的可验证声明的目标记录信息；

若根据所述目标记录信息中的有效性字段，确定所述待验证的可验证声明处于有效状态，则根据所述用户的数字身份信息，发送业务确认请求给所述授权应用，并确定是否通过所述授权应用获取到所述用户的确认信息；以及，

根据所述目标记录信息确定所述待验证的可验证声明是否合法；

若获取到所述用户的确认信息且确定所述待验证的可验证声明合法，则确定所述待验证的可验证声明验证通过。

13、根据权利要求 11 所述的方法，所述待验证的可验证声明包括：声明标识；所述区块链中存储的关于所述待验证的可验证声明的记录信息包括：有效性字段；

根据所述区块链中存储的关于所述待验证的可验证声明的记录信息，对所述待验证的可验证声明进行验证，包括：

从所述区块链存储的记录信息中，根据所述声明标识，查询关于所述待验证的可验证声明的目标记录信息；

若根据所述目标记录信息中的有效性字段，确定所述待验证的可验证声明处于有效状态，则根据所述目标记录信息确定所述待验证的可验证声明是否合法；

若确定所述待验证的可验证声明合法，则确定所述待验证的可验证声明验证通过。

14、根据权利要求 12 或 13 所述的方法，所述待验证的可验证声明包括：签名信息和创建平台的数字身份信息，所述目标记录信息包括：创建记录信息；

根据所述目标记录信息确定所述待验证的可验证声明是否合法，包括：

根据所述创建平台的数字身份信息，获取所述创建平台的公钥，采用所述创建平台

的公钥对所述签名信息进行验证；以及，

计算所述待验证的可验证声明中的第二指定信息的哈希值，并获取所述创建记录信息中的所述可验证声明对应的哈希值，将计算的所述第二指定信息的哈希值与所述可验证声明对应的哈希值进行匹配；

若所述签名信息验证通过，且所述哈希值匹配成功，则确定所述待验证的可验证声明合法。

15、根据权利要求 12 或 13 所述的方法，所述待验证的可验证声明包括：签名信息和创建平台的数字身份信息；所述目标记录信息包括：创建记录信息；

根据所述目标记录信息确定所述待验证的可验证声明是否合法，包括：

根据所述创建平台的数字身份信息，获取所述创建平台的公钥，采用所述创建平台的公钥对所述签名信息进行验证；以及，

将所述待验证的可验证声明与所述创建记录信息中的可验证声明进行匹配；

若匹配成功且所述签名信息验证通过，则确定所述待验证的可验证声明合法。

16、一种基于区块链的可验证声明的创建装置，应用于可验证声明的创建平台，包括：

接收模块，其接收授权应用发送的创建请求，其中，所述创建请求为所述授权应用响应于用户的可验证声明申请操作而发送，所述创建请求包括：待创建的可验证声明的声明内容和所述用户的数字身份信息；

创建模块，其根据所述声明内容和所述数字身份信息，创建可验证声明；

发送模块，其向所述授权应用发送所述可验证声明；

生成模块，其生成所述可验证声明的创建记录信息，向区块链中的至少一个区块链节点发送所述创建记录信息，以使所述区块链节点将所述创建记录信息保存至区块链中。

17、根据权利要求 16 所述的装置，其中，

所述创建模块，确定创建所述可验证声明所需的字段信息；以及，

根据所述字段信息、所述声明内容、所述用户的数字身份信息及所述创建平台的数字身份信息，创建可验证声明。

18、根据权利要求 17 所述的装置，其中，

所述创建模块，生成所述可验证声明的声明标识；以及，

采用所述创建平台的私钥对预设的第一指定信息进行签名，得到签名数据；

将所述声明标识和所述签名数据作为创建所述可验证声明所需的字段信息。

19、根据权利要求 18 所述的装置，其中，

所述生成模块，计算所述用户的数字身份信息的哈希值；以及，

计算所述创建平台的数字身份信息的哈希值；

计算所述可验证声明中第二指定信息的哈希值；

将计算的各个所述哈希值、所述声明标识、有效性字段进行关联记录，并将记录的信息作为所述可验证声明的创建记录信息；其中，所述有效性字段表征所述可验证声明所处的状态。

20、一种可验证声明的创建装置，应用于授权应用，包括：

获取模块，其响应于用户的可验证声明申请操作，获取待创建的可验证声明的声明内容；

发送模块，其根据所述声明内容和所述用户的数字身份信息，向创建平台发送创建请求，以使所述创建平台根据所述声明内容和所述用户的数字身份信息，创建可验证声明；

接收模块，其接收所述创建平台发送的所述可验证声明。

21、一种基于区块链的可验证声明的创建装置，应用于区块链中的区块链节点，包括：

接收模块，其接收创建平台发送的可验证声明的创建记录信息，其中，所述创建记录信息为所述创建平台根据授权应用发送的创建请求，创建所述可验证声明之后所生成的信息；

保存模块，其将所述创建记录信息保存至区块链中。

22、根据权利要求 21 所述的装置，所述装置还包括：

验证模块，接收第三方发送的声明验证请求，其中，所述声明验证请求包括待验证的可验证声明，所述第三方在所述可验证声明验证通过时，基于所述可验证声明进行业务处理；

调用部署于所述区块链中的智能合约，根据所述区块链中存储的关于所述待验证的可验证声明的记录信息，对所述待验证的可验证声明进行验证。

23、一种基于区块链的可验证声明的创建系统，包括：授权应用、创建平台和区块链；

所述授权应用，响应于用户的可验证声明申请操作，获取待创建的可验证声明的声明内容，根据所述声明内容和所述用户的数字身份信息，向所述创建平台发送创建请求；

所述创建平台，根据所述声明内容和所述数字身份信息，创建可验证声明，向所述授权应用发送所述可验证声明；以及，生成所述可验证声明的创建记录信息，将所述创

建记录信息发送给所述区块链中的至少一个区块链节点；

所述区块链中的区块链节点，在接收到所述创建记录信息时，将所述创建记录信息保存至区块链中。

24、一种基于区块链的可验证声明的创建设备，包括：

处理器；以及，

被安排成存储计算机可执行指令的存储器，所述计算机可执行指令在被执行时使所述处理器：

接收授权应用发送的创建请求，其中，所述创建请求为所述授权应用响应于用户的可验证声明申请操作而发送，所述创建请求包括：待创建的可验证声明的声明内容和所述用户的数字身份信息；

根据所述声明内容和所述数字身份信息，创建可验证声明；

向所述授权应用发送所述可验证声明；

生成所述可验证声明的创建记录信息，向区块链中的至少一个区块链节点发送所述创建记录信息，以使所述区块链节点将所述创建记录信息保存至区块链中。

25、一种基于区块链的可验证声明的创建设备，包括：

处理器；以及，

被安排成存储计算机可执行指令的存储器，所述计算机可执行指令在被执行时使所述处理器：

响应于用户的可验证声明申请操作，获取待创建的可验证声明的声明内容；

根据所述声明内容和所述用户的数字身份信息，向创建平台发送创建请求，以使所述创建平台根据所述声明内容和所述用户的数字身份信息，创建可验证声明；

接收所述创建平台发送的所述可验证声明。

26、一种基于区块链的可验证声明的创建设备，包括：

接收创建平台发送的可验证声明的创建记录信息，其中，所述创建记录信息为所述创建平台根据授权应用发送的创建请求，创建所述可验证声明之后所生成的信息；

将所述创建记录信息保存至区块链中。

27、一种存储介质，用于存储计算机可执行指令，所述计算机可执行指令在被执行时实现以下流程：

接收授权应用发送的创建请求，其中，所述创建请求为所述授权应用响应于用户的可验证声明申请操作而发送，所述创建请求包括：待创建的可验证声明的声明内容和所述用户的数字身份信息；

根据所述声明内容和所述数字身份信息，创建可验证声明；

向所述授权应用发送所述可验证声明；

生成所述可验证声明的创建记录信息，向区块链中的至少一个区块链节点发送所述创建记录信息，以使所述区块链节点将所述创建记录信息保存至区块链中。

28、一种存储介质，用于存储计算机可执行指令，所述计算机可执行指令在被执行时实现以下流程：

响应于用户的可验证声明申请操作，获取待创建的可验证声明的声明内容；

根据所述声明内容和所述用户的数字身份信息，向创建平台发送创建请求，以使所述创建平台根据所述声明内容和所述用户的数字身份信息，创建可验证声明；

接收所述创建平台发送的所述可验证声明。

29、一种存储介质，用于存储计算机可执行指令，所述计算机可执行指令在被执行时实现以下流程：

接收创建平台发送的可验证声明的创建记录信息，其中，所述创建记录信息为所述创建平台根据授权应用发送的创建请求，创建所述可验证声明之后所生成的信息；

将所述创建记录信息保存至区块链中。

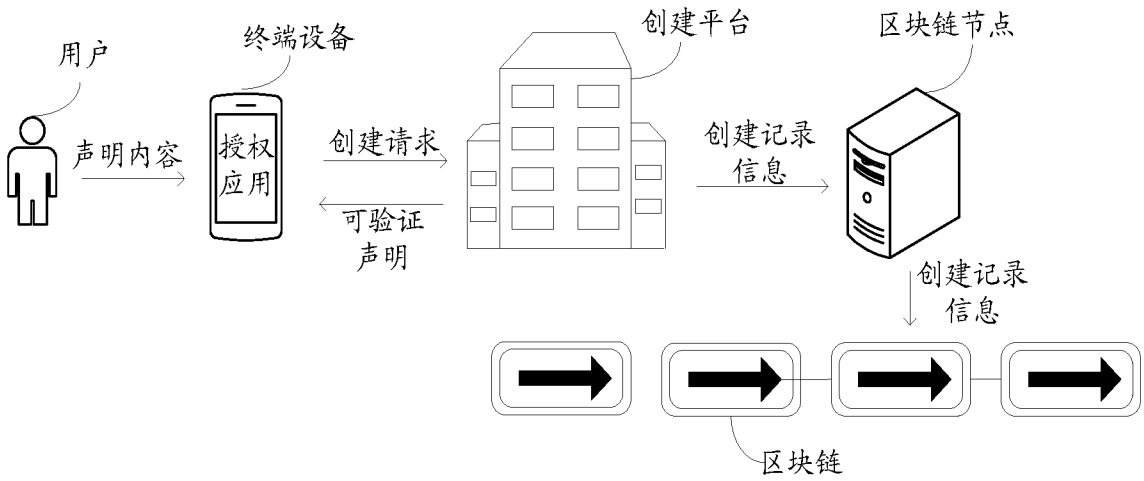

用户
终端设备
创建平台
区块链节点
声明内容
授权应用
创建请求
可验证声明
创建记录信息
创建记录信息
区块链

图 1

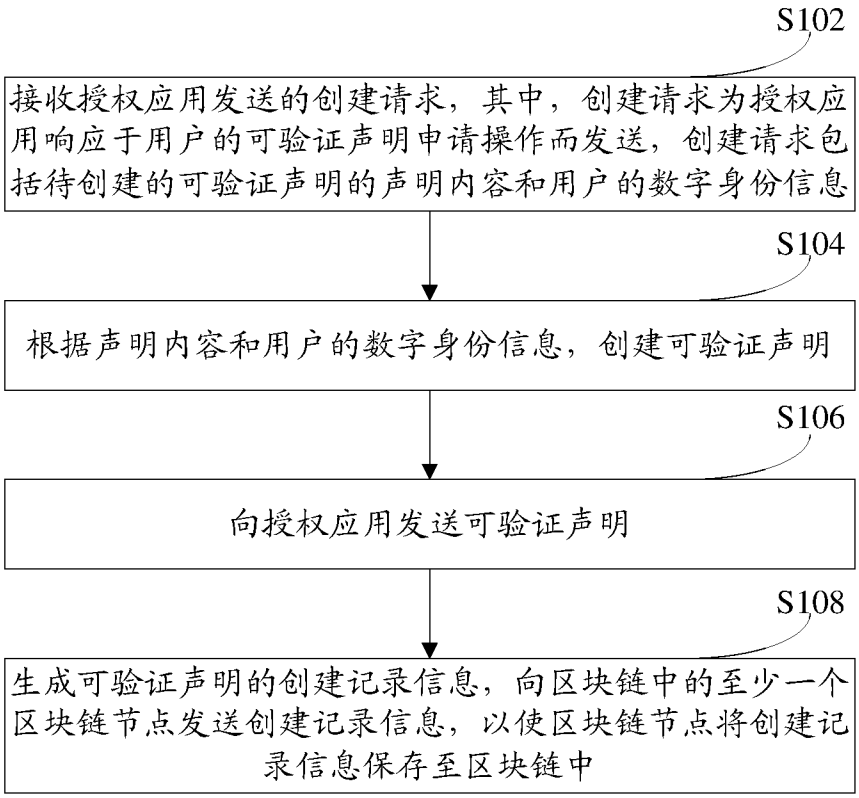

S102
接收授权应用发送的创建请求，其中，创建请求为授权应用响应于用户的可验证声明申请操作而发送，创建请求包括待创建的可验证声明的声明内容和用户的数字身份信息
S104
根据声明内容和用户的数字身份信息，创建可验证声明
S106
向授权应用发送可验证声明
S108
生成可验证声明的创建记录信息，向区块链中的至少一个区块链节点发送创建记录信息，以使区块链节点将创建记录信息保存至区块链中

图 2

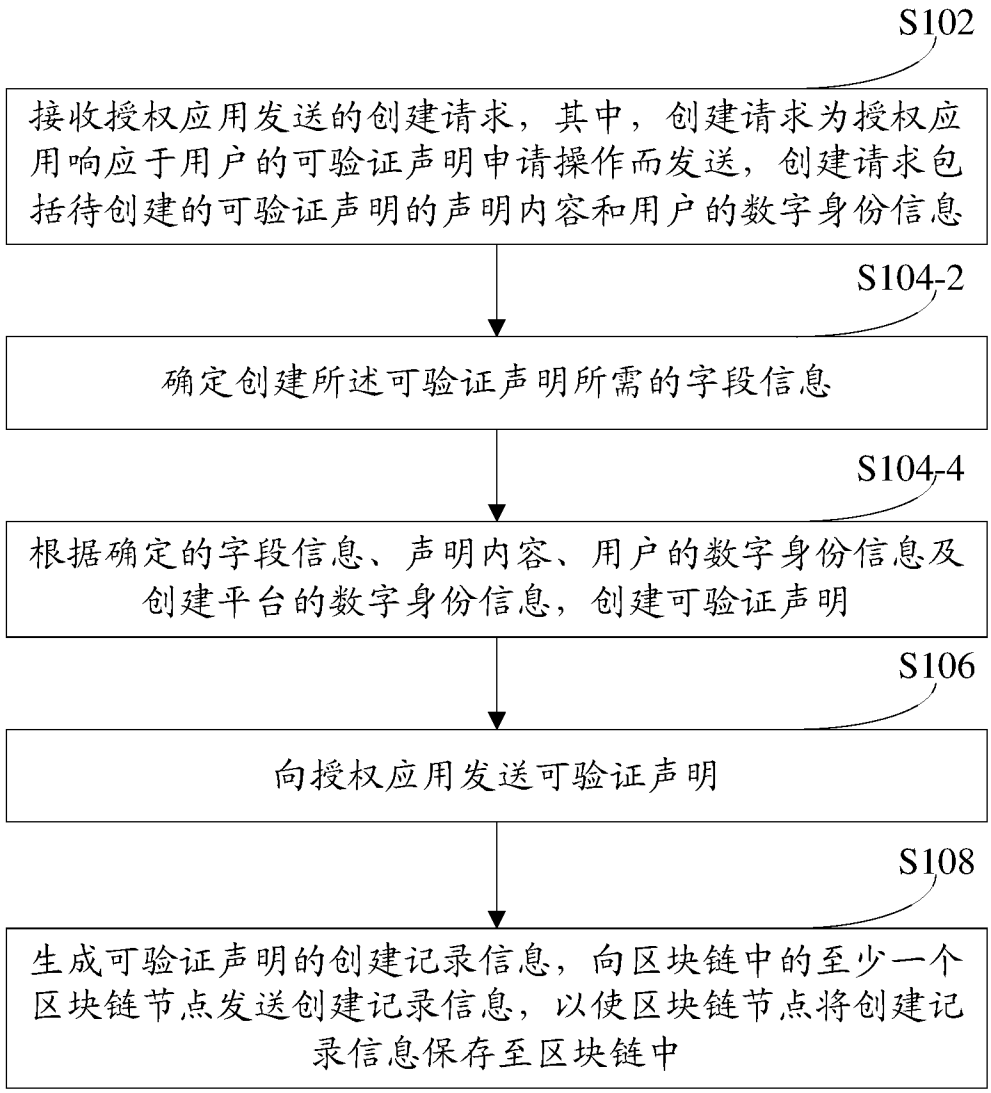

S102
接收授权应用发送的创建请求，其中，创建请求为授权应用响应于用户的可验证声明申请操作而发送，创建请求包括待创建的可验证声明的声明内容和用户的数字身份信息
S104-2
确定创建所述可验证声明所需的字段信息
S104-4
根据确定的字段信息、声明内容、用户的数字身份信息及创建平台的数字身份信息，创建可验证声明
S106
向授权应用发送可验证声明
S108
生成可验证声明的创建记录信息，向区块链中的至少一个区块链节点发送创建记录信息，以使区块链节点将创建记录信息保存至区块链中

图 3

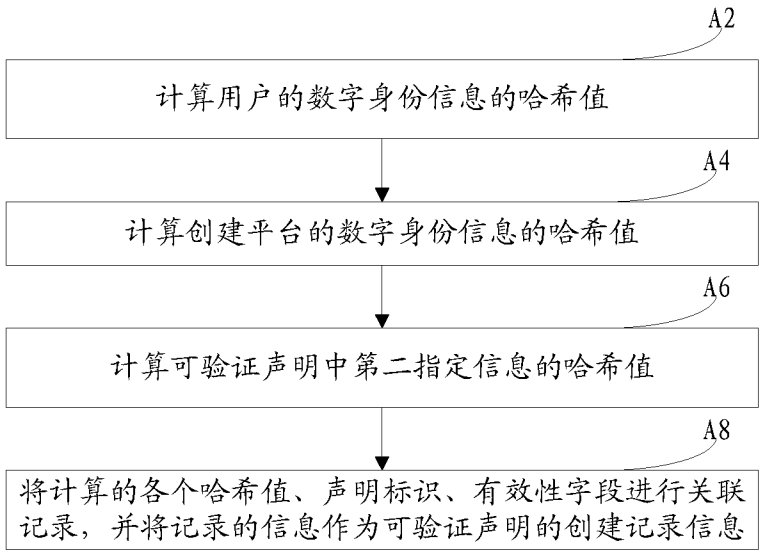

A2
计算用户的数字身份信息的哈希值
A4
计算创建平台的数字身份信息的哈希值
A6
计算可验证声明中第二指定信息的哈希值
A8
将计算的各个哈希值、声明标识、有效性字段进行关联记录，并将记录的信息作为可验证声明的创建记录信息

图 4

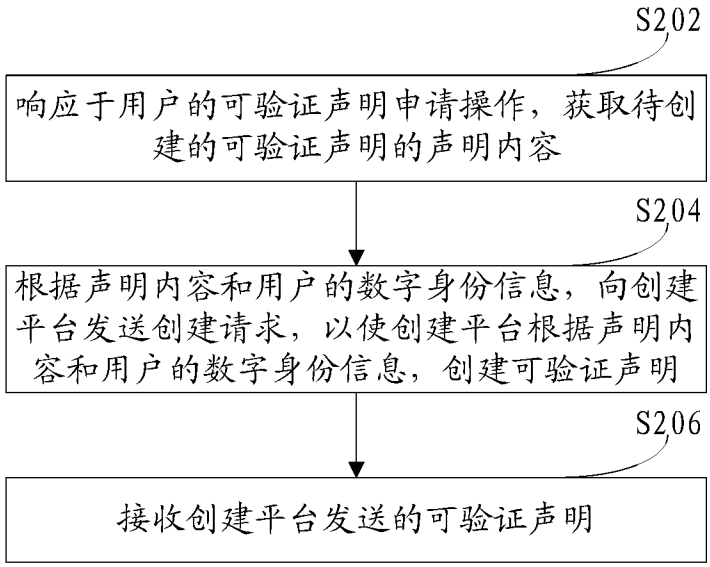

S202
响应于用户的可验证声明申请操作，获取待创建的可验证声明的声明内容
S204
根据声明内容和用户的数字身份信息，向创建平台发送创建请求，以使创建平台根据声明内容和用户的数字身份信息，创建可验证声明
S206
接收创建平台发送的可验证声明

图 5

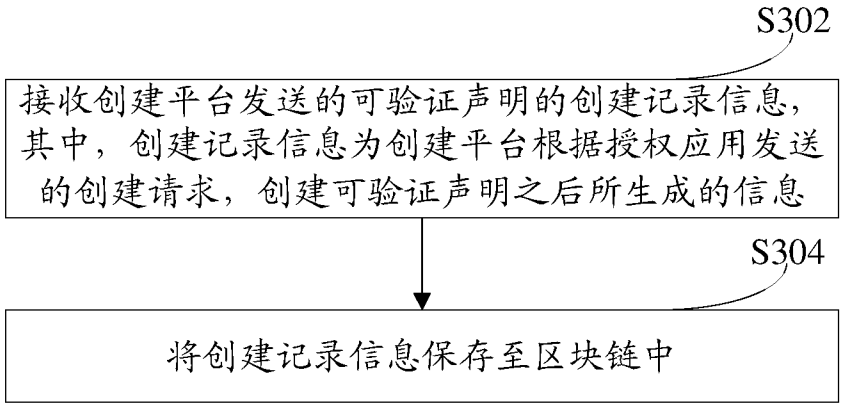

S302
接收创建平台发送的可验证声明的创建记录信息，其中，创建记录信息为创建平台根据授权应用发送的创建请求，创建可验证声明之后所生成的信息
S304
将创建记录信息保存至区块链中

图 6

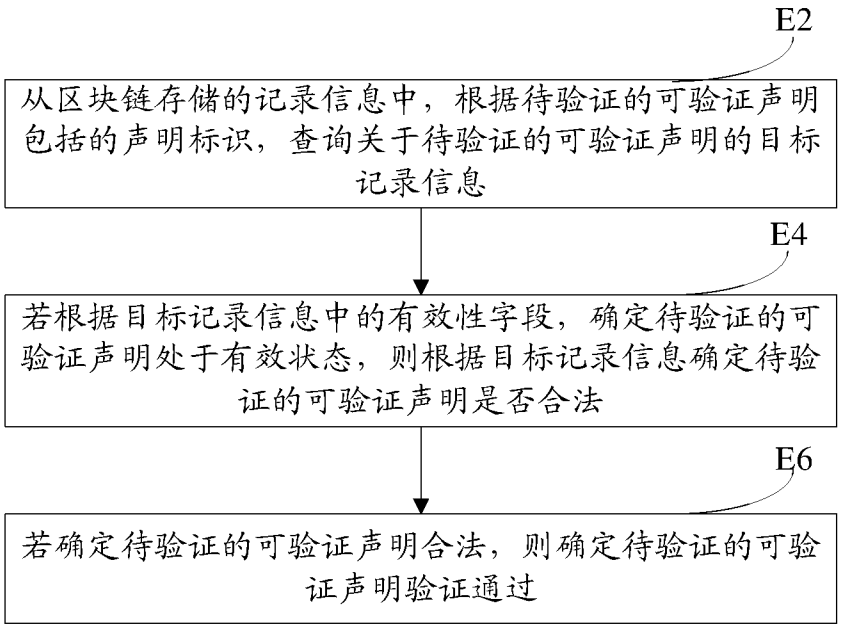

E2
从区块链存储的记录信息中，根据待验证的可验证声明包括的声明标识，查询关于待验证的可验证声明的目标记录信息
E4
若根据目标记录信息中的有效性字段，确定待验证的可验证声明处于有效状态，则根据目标记录信息确定待验证的可验证声明是否合法
E6
若确定待验证的可验证声明合法，则确定待验证的可验证声明验证通过

图 7

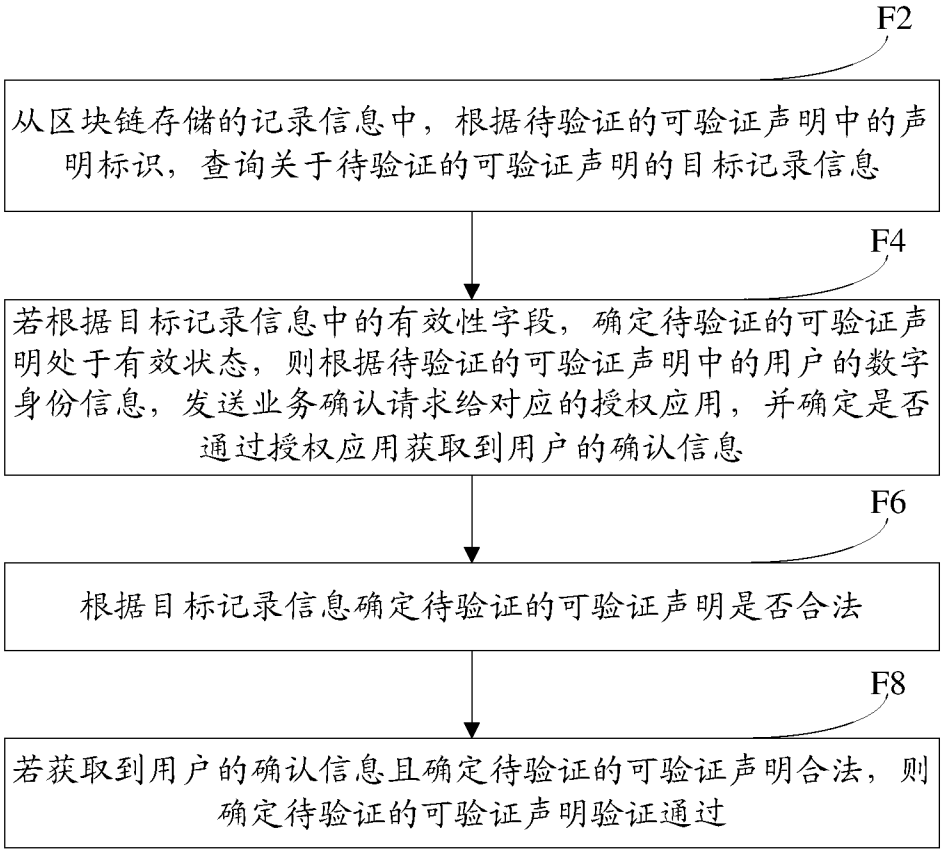

F2
从区块链存储的记录信息中，根据待验证的可验证声明中的声明标识，查询关于待验证的可验证声明的目标记录信息
F4
若根据目标记录信息中的有效性字段，确定待验证的可验证声明处于有效状态，则根据待验证的可验证声明中的用户的数字身份信息，发送业务确认请求给对应的授权应用，并确定是否通过授权应用获取到用户的确认信息
F6
根据目标记录信息确定待验证的可验证声明是否合法
F8
若获取到用户的确认信息且确定待验证的可验证声明合法，则确定待验证的可验证声明验证通过

图 8

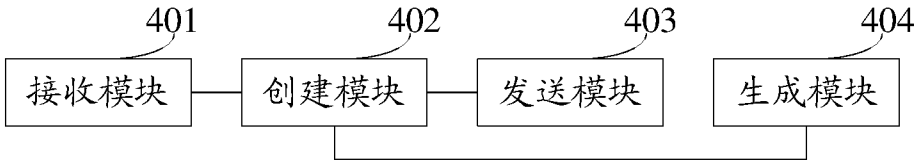

401
402
403
404
接收模块
创建模块
发送模块
生成模块

图 9

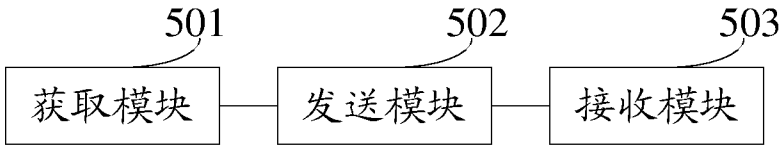

501
502
503
获取模块
发送模块
接收模块

图 10

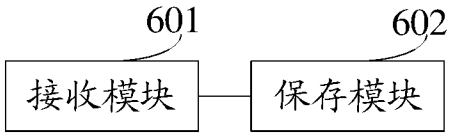

601
602
接收模块
保存模块

图 11

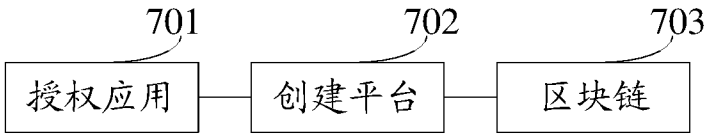

701
702
703
授权应用
创建平台
区块链

图 12

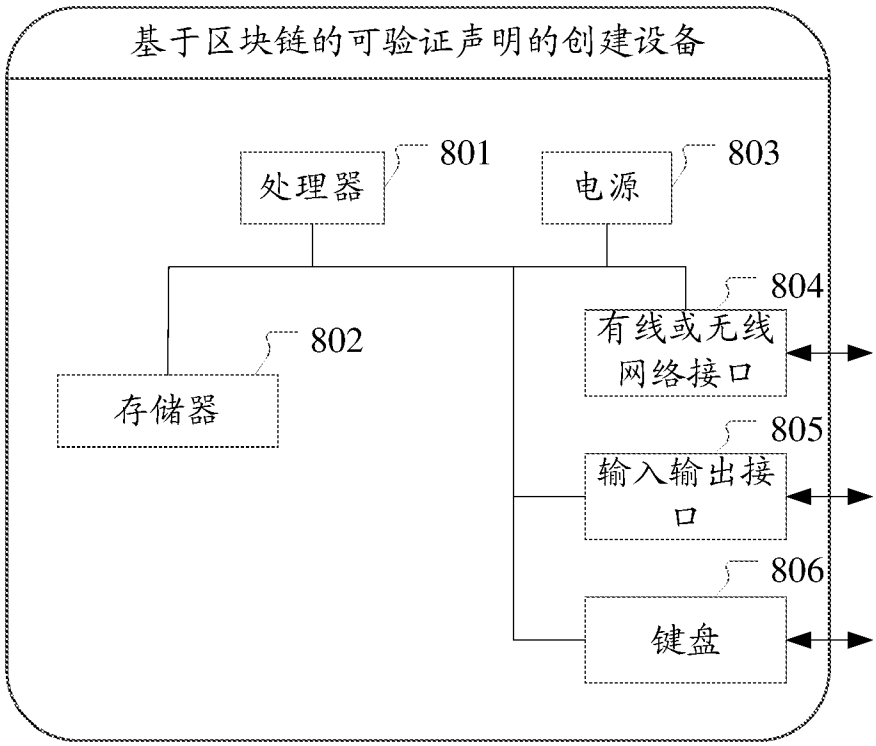

基于区块链的可验证声明的创建设备
处理器
801
电源
803
804
有线或无线网络接口
802
存储器
805
输入输出接口
806
键盘

图 13

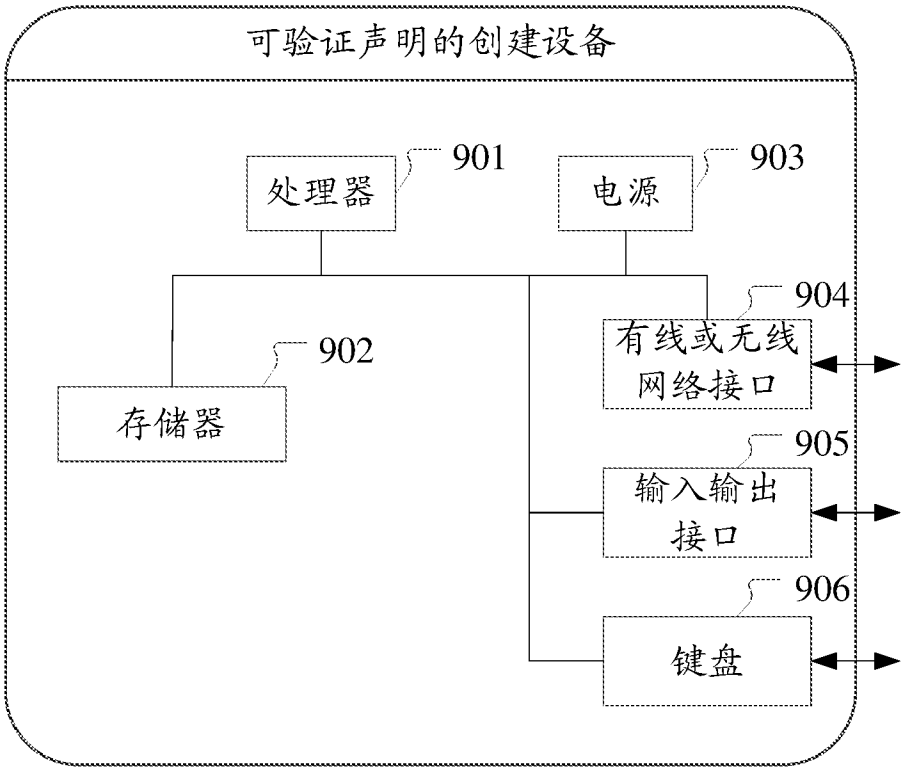

可验证声明的创建设备
处理器
901
电源
903
904
有线或无线
网络接口
902
存储器
905
输入输出
接口
906
键盘

图 14

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2020/107903

A. CLASSIFICATION OF SUBJECT MATTER

G06F 16/27(2019.01)i; G06Q 30/00(2012.01)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; G06Q

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)

WPI, EPODOC, CNKI, CNPAT, IEEE, GOOGLE: 区块链, 可验证, 声明, 创建, 请求, 服务器, 客户端, 终端, block, chain, verifiable, claim, create, generate, request, server, client, terminal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110795501 A (ALIPAY (HANGZHOU) INFORMATION TECHNOLOGY CO., LTD.) 14 February 2020 (2020-02-14) claims 1-29	1-29
X	WO 2019179535 A2 (ALIBABA GROUP HOLDING LIMITED) 26 September 2019 (2019-09-26) description, paragraphs 66-70, 106-111, figures 3, 13	1-29
A	CN 109274652 A (TENCENT TECHNOLOGY SHENZHEN CO., LTD.) 25 January 2019 (2019-01-25) entire document	1-29
A	US 2019013931 A1 (AWARE, INC.) 10 January 2019 (2019-01-10) entire document	1-29

☐ 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 October 2020	**10 November 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/CN2020/107903

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	110795501	A	14 February 2020	None			
WO	2019179535	A2	26 September 2019	CN	111095327	A	01 May 2020
				EP	3688633	A2	05 August 2020
				US	2020127845	A1	23 April 2020
CN	109274652	A	25 January 2019	None			
US	2019013931	A1	10 January 2019	WO	2017044554	A1	16 March 2017
				US	2020252203	A1	06 August 2020
				EP	3348019	A1	18 July 2018

国际检索报告

国际申请号
PCT/CN2020/107903

A. 主题的分类

G06F 16/27(2019.01)i; G06Q 30/00(2012.01)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; G06Q

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））

WPI, EPODOC, CNKI, CNPAT, IEEE, GOOGLE: 区块链, 可验证, 声明, 创建, 请求, 服务器, 客户端, 终端, block, chain, verifiable, claim, create, generate, request, server, client, terminal

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 110795501 A (支付宝杭州信息技术有限公司) 2020年 2月 14日 (2020-02-14) 权利要求1-29	1-29
X	WO 2019179535 A2 (ALIBABA GROUP HOLDING LIMITED) 2019年 9月 26日 (2019-09-26) 说明书第66-70, 106-111段, 附图3, 13	1-29
A	CN 109274652 A (腾讯科技深圳有限公司) 2019年 1月 25日 (2019-01-25) 全文	1-29
A	US 2019013931 A1 (AWARE, INC.) 2019年 1月 10日 (2019-01-10) 全文	1-29

☐ 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 10月 27日	2020年 11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 王艳臣 电话号码 86-(10)-53961435

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2020/107903

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	110795501	A	2020年 2月 14日		无		
WO	2019179535	A2	2019年 9月 26日	CN	111095327	A	2020年 5月 1日
				EP	3688633	A2	2020年 8月 5日
				US	2020127845	A1	2020年 4月 23日
CN	109274652	A	2019年 1月 25日		无		
US	2019013931	A1	2019年 1月 10日	WO	2017044554	A1	2017年 3月 16日
				US	2020252203	A1	2020年 8月 6日
				EP	3348019	A1	2018年 7月 18日