



# (12) 发明专利申请

(10) 申请公布号 CN 115438386 A

(43) 申请公布日 2022. 12. 06

(21) 申请号 202211056178.9

G06Q 40/00 (2012.01)

(22) 申请日 2022.08.31

G06Q 50/26 (2012.01)

(71) 申请人 中国工商银行股份有限公司

地址 100140 北京市西城区复兴门内大街  
55号

申请人 工银科技有限公司

(72) 发明人 秦日臻

(74) 专利代理机构 北京康信知识产权代理有限  
责任公司 11240

专利代理师 周春枚

(51) Int. Cl.

G06F 21/64 (2013.01)

G06F 21/62 (2013.01)

G06F 21/60 (2013.01)

H04L 67/1097 (2022.01)

权利要求书2页 说明书12页 附图2页

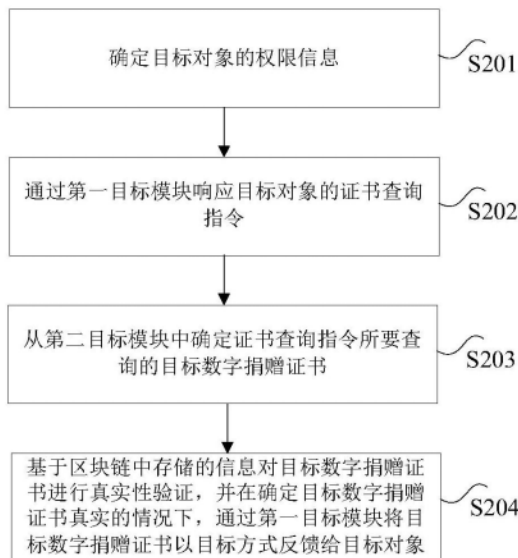
## (54) 发明名称

基于区块链的证书管理方法、装置及电子设备

## (57) 摘要

本发明公开了一种基于区块链的证书管理方法、装置及电子设备。涉及区块链领域,该方法包括:确定目标对象的权限信息,并依据权限信息确定第一目标模块;通过第一目标模块响应目标对象的证书查询指令;从第二目标模块中确定证书查询指令所要查询的目标数字捐赠证书,第二目标模块用于存储目标数字捐赠证书;基于区块链中存储的信息对目标数字捐赠证书进行真实性验证,并在确定目标数字捐赠证书真实的情况下,通过第一目标模块将目标数字捐赠证书以目标方式反馈给目标对象,其中,区块链至少用于存储数字捐赠证书对应的哈希值,第一目标模块与目标方式相对应。本发明解决了现有技术中由于纸质的捐赠证书易伪造所造成的证书真实性低的技术问题。

CN 115438386 A



1. 一种基于区块链的证书管理方法,其特征在于,包括:

确定目标对象的权限信息,并依据所述权限信息确定第一目标模块;

通过所述第一目标模块响应所述目标对象的证书查询指令;

从第二目标模块中确定所述证书查询指令所要查询的目标数字捐赠证书,其中,所述第二目标模块用于存储所述目标数字捐赠证书;

基于区块链中存储的信息对所述目标数字捐赠证书进行真实性验证,并在确定所述目标数字捐赠证书真实的情况下,通过所述第一目标模块将所述目标数字捐赠证书以目标方式反馈给所述目标对象,其中,所述区块链至少用于存储数字捐赠证书对应的哈希值,所述第一目标模块与所述目标方式相对应。

2. 根据权利要求1所述的方法,其特征在于,在确定目标对象的权限信息之前,所述方法还包括:

获取捐赠对象向目标机构进行捐赠的捐赠信息;

基于所述捐赠信息生成数字捐赠证书,并生成与所述数字捐赠证书对应的哈希值;

将与所述数字捐赠证书对应的哈希值以及所述捐赠信息存储到所述区块链中。

3. 根据权利要求2所述的方法,其特征在于,基于所述捐赠信息生成数字捐赠证书,包括:

获取所述捐赠对象发送的目标证书格式;

基于所述捐赠信息以及所述目标证书格式生成所述数字捐赠证书。

4. 根据权利要求1所述的方法,其特征在于,基于区块链中存储的信息对所述目标数字捐赠证书进行真实性验证,包括:

计算与所述目标数字捐赠证书对应的哈希值;

从所述区块链中确定与所述证书查询指令中的查询信息对应的第一目标哈希值;

在所述目标数字捐赠证书对应的哈希值与所述第一目标哈希值相同的情况下,确定所述目标数字捐赠证书真实;

在所述目标数字捐赠证书对应的哈希值与所述第一目标哈希值不同的情况下,确定所述目标数字捐赠证书异常。

5. 根据权利要求1所述的方法,其特征在于,确定目标对象的权限信息,并依据所述权限信息确定第一目标模块,包括:

若所述目标对象的权限信息为第一权限信息,则确定所述目标对象为第一目标对象,并将证书查询模块确定为所述第一目标模块;

若所述目标对象的权限信息为第二权限信息,则确定所述目标对象为第二目标对象,并将证书展示模块确定为所述第一目标模块,其中,所述第一权限信息所表征的权限高于所述第二权限信息所表征的权限。

6. 根据权利要求5所述的方法,其特征在于,通过所述第一目标模块将所述目标数字捐赠证书以目标方式反馈给所述目标对象,包括:

当所述第一目标模块为所述证书查询模块时,将所述目标数字捐赠证书发送给所述第一目标对象;

当所述第一目标模块为所述证书展示模块,向所述第二目标对象展示所述目标数字捐赠证书。

7. 根据权利要求6所述的方法,其特征在于,在向所述第二目标对象展示所述目标数字捐赠证书之后,所述方法还包括:

响应第三目标对象的目标证书查询指令,并基于所述目标证书查询指令确定目标查询信息,其中,所述第三目标对象用于为所述第二目标对象办理待办业务,所述目标查询信息至少包括所述第二目标对象所提供的目标标识以及第二目标哈希值;

从所述区块链中确定与所述目标标识对应的第三目标哈希值;

比对所述第二目标哈希值与所述第三目标哈希值是否相同,并将比对结果反馈给所述第三目标对象,其中,所述比对结果用于所述第三目标对象确定是否为所述第二目标对象办理所述待办业务。

8. 一种基于区块链的证书管理装置,其特征在于,包括:

第一确定模块,用于确定目标对象的权限信息,并依据所述权限信息确定第一目标模块;

响应模块,用于通过所述第一目标模块响应所述目标对象的证书查询指令;

第二确定模块,用于从第二目标模块中确定所述证书查询指令所要查询的目标数字捐赠证书,其中,所述第二目标模块用于存储所述目标数字捐赠证书;

反馈模块,用于基于区块链中存储的信息对所述目标数字捐赠证书进行真实性验证,并在确定所述目标数字捐赠证书真实的情况下,通过所述第一目标模块将所述目标数字捐赠证书以目标方式反馈给所述目标对象,其中,所述区块链至少用于存储数字捐赠证书对应的哈希值,所述第一目标模块与所述目标方式相对应。

9. 一种计算机可读存储介质,其特征在于,所述计算机可读存储介质中存储有计算机程序,其中,所述计算机程序被设置为运行时执行所述权利要求1至7任一项中所述的基于区块链的证书管理方法。

10. 一种电子设备,其特征在于,所述电子设备包括一个或多个处理器;存储器,用于存储一个或多个程序,当所述一个或多个程序被所述一个或多个处理器执行时,使得所述一个或多个处理器实现用于运行程序,其中,所述程序被设置为运行时执行所述权利要求1至7任一项中所述的基于区块链的证书管理方法。

## 基于区块链的证书管理方法、装置及电子设备

### 技术领域

[0001] 本发明涉及区块链领域,具体而言,涉及一种基于区块链的证书管理方法、装置及电子设备。

### 背景技术

[0002] 为了帮助社会中各类弱势群体,组织社会各界爱心人士为其提供无偿的人道主义救援,我国成立了各种类型的非营利性的慈善公益组织。在经济和物质上有余力的任何人士,都可以通过法定认可的慈善组织向需要帮扶的群体伸出援手,通常慈善机构会授予捐赠者证书来作为对捐赠行为的鼓励和证明。某些情况下,民众的捐赠行为可以获得一定的扣税优惠等。

[0003] 目前,慈善机构的工作大多还是在线下人工开展,捐赠资金的往来、捐赠受捐主体的管理等多以纸质化形式进行,给捐赠者出具的捐赠证书也多以纸质证书的形式存在,从而使得捐赠证书在实际应用中存在一些问题。例如,纸质证书和电子证书易伪造,采信度低,办事机构较难鉴定证书的真实性,使用者有时得搭配各种材料证明证书的真实性和有效性,此外,也纸质证书不方便携带和存储,进而限制了捐赠证书的使用范围。

[0004] 针对上述的问题,目前尚未提出有效的解决方案。

### 发明内容

[0005] 本发明实施例提供了一种基于区块链的证书管理方法、装置及电子设备,以至少解决现有技术中由于纸质的捐赠证书易伪造所造成的证书真实性低的技术问题。

[0006] 根据本发明实施例的一个方面,提供了一种基于区块链的证书管理方法,包括:确定目标对象的权限信息,并依据权限信息确定第一目标模块;通过第一目标模块响应目标对象的证书查询指令;从第二目标模块中确定证书查询指令所要查询的目标数字捐赠证书,其中,第二目标模块用于存储目标数字捐赠证书;基于区块链中存储的信息对目标数字捐赠证书进行真实性验证,并在确定目标数字捐赠证书真实的情况下,通过第一目标模块将目标数字捐赠证书以目标方式反馈给目标对象,其中,区块链至少用于存储数字捐赠证书对应的哈希值,第一目标模块与目标方式相对应。

[0007] 进一步地,基于区块链的证书管理方法还包括:在确定目标对象的权限信息之前,获取捐赠对象向目标机构进行捐赠的捐赠信息;基于捐赠信息生成数字捐赠证书,并生成与数字捐赠证书对应的哈希值;将与数字捐赠证书对应的哈希值以及捐赠信息存储到区块链中。

[0008] 进一步地,基于区块链的证书管理方法还包括:获取捐赠对象发送的目标证书格式;基于捐赠信息以及目标证书格式生成数字捐赠证书。

[0009] 进一步地,基于区块链的证书管理方法还包括:计算与目标数字捐赠证书对应的哈希值;从区块链中确定与证书查询指令中的查询信息对应的第一目标哈希值;在目标数字捐赠证书对应的哈希值与第一目标哈希值相同的情况下,确定目标数字捐赠证书真实;

在目标数字捐赠证书对应的哈希值与第一目标哈希值不同的情况下,确定目标数字捐赠证书异常。

[0010] 进一步地,基于区块链的证书管理方法还包括:若目标对象的权限信息为第一权限信息,则确定目标对象为第一目标对象,并将证书查询模块确定为第一目标模块;若目标对象的权限信息为第二权限信息,则确定目标对象为第二目标对象,并将证书展示模块确定为第一目标模块,其中,第一权限信息所表征的权限高于第二权限信息所表征的权限。

[0011] 进一步地,基于区块链的证书管理方法还包括:当第一目标模块为证书查询模块时,将目标数字捐赠证书发送给第一目标对象;当第一目标模块为证书展示模块,向第二目标对象展示目标数字捐赠证书。

[0012] 进一步地,基于区块链的证书管理方法还包括:在向第二目标对象展示目标数字捐赠证书之后,响应第三目标对象的目标证书查询指令,并基于目标证书查询指令确定目标查询信息,其中,第三目标对象用于为第二目标对象办理待办业务,目标查询信息至少包括第二目标对象所提供的目标标识以及第二目标哈希值;从区块链中确定与目标标识对应的第三目标哈希值;比对第二目标哈希值与第三目标哈希值是否相同,并将比对结果反馈给第三目标对象,其中,比对结果用于第三目标对象确定是否为第二目标对象办理待办业务。

[0013] 根据本发明实施例的另一方面,还提供了一种基于区块链的证书管理装置,包括:第一确定模块,用于确定目标对象的权限信息,并依据权限信息确定第一目标模块;响应模块,用于通过第一目标模块响应目标对象的证书查询指令;第二确定模块,用于从第二目标模块中确定证书查询指令所要查询的目标数字捐赠证书,其中,第二目标模块用于存储目标数字捐赠证书;反馈模块,用于基于区块链中存储的信息对目标数字捐赠证书进行真实性验证,并在确定目标数字捐赠证书真实的情况下,通过第一目标模块将目标数字捐赠证书以目标方式反馈给目标对象,其中,区块链至少用于存储数字捐赠证书对应的哈希值,第一目标模块与目标方式相对应。

[0014] 根据本发明实施例的另一方面,还提供了一种计算机可读存储介质,计算机可读存储介质中存储有计算机程序,其中,计算机程序被设置为运行时执行上述的基于区块链的证书管理方法。

[0015] 根据本发明实施例的另一方面,还提供了一种电子设备,电子设备包括一个或多个处理器;存储器,用于存储一个或多个程序,当一个或多个程序被一个或多个处理器执行时,使得一个或多个处理器实现用于运行程序,其中,程序被设置为运行时执行上述的基于区块链的证书管理方法。

[0016] 在本发明实施例中,采用基于区块链中存储的信息对目标对象所要查询的证书进行真实性验证,并在验证成功后将证书反馈给目标对象的方式,通过确定目标对象的权限信息,并依据权限信息确定第一目标模块,然后通过第一目标模块响应目标对象的证书查询指令,接着从第二目标模块中确定证书查询指令所要查询的目标数字捐赠证书,从而基于区块链中存储的信息对目标数字捐赠证书进行真实性验证,并在确定目标数字捐赠证书真实的情况下,通过第一目标模块将目标数字捐赠证书以目标方式反馈给目标对象。其中,第二目标模块用于存储目标数字捐赠证书,区块链至少用于存储数字捐赠证书对应的哈希值,第一目标模块与目标方式相对应。

[0017] 在上述过程中,由于区块链能够有效保证其所存储的信息不可篡改、不可伪造、不可抵赖、可全程留痕,因此,通过将数字捐赠证书的哈希值存储到区块链中,并在将目标对象所查询的目标数字捐赠证书反馈给目标对象之前,基于区块链中的存储的哈希值对第二目标模块中的目标数字捐赠证书进行真实性验证,可以有效保证验证结果的有效性,从而保证了发送给目标对象的目标数字捐赠证书的真实性,避免了现有技术中纸质捐赠证书易伪造的问题。此外,通过基于目标对象权限的不同,采用不同的方式反馈目标对象所要查询的数字捐赠证书,避免了基于相同的方式向不同的目标对象反馈目标数字捐赠证书造成的可信度低的对象对直接获取的目标数字捐赠证书容易伪造或是可信度高的对象对图片形式的目标数字捐赠证书难以留存的现象,从而更进一步地保证了捐赠证书的真实性。

[0018] 由此可见,本申请所提供的方案达到了基于区块链中存储的信息对目标对象所要查询的证书进行真实性验证,并在验证成功后将证书反馈给目标对象的目的,从而实现了提高捐赠证书真实性的技术效果,进而解决了现有技术中由于纸质的捐赠证书易伪造所造成的证书真实性低的技术问题。

### 附图说明

[0019] 此处所说明的附图用来提供对本发明的进一步理解,构成本申请的一部分,本发明的示意性实施例及其说明用于解释本发明,并不构成对本发明的不当限定。在附图中:

[0020] 图1是根据本发明实施例的一种可选的证书管理系统的示意图;

[0021] 图2是根据本发明实施例的一种可选的证书管理方法的示意图;

[0022] 图3是根据本发明实施例的一种可选的证书管理方法的应用流程图;

[0023] 图4是根据本发明实施例的一种可选的证书管理装置的示意图;

[0024] 图5是根据本发明实施例的一种可选的电子设备的示意图。

### 具体实施方式

[0025] 为了使本技术领域的人员更好地理解本发明方案,下面将结合本发明实施例中的附图,对本发明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发明一部分的实施例,而不是全部的实施例。基于本发明中的实施例,本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例,都应当属于本发明保护的范围。

[0026] 需要说明的是,本发明的说明书和权利要求书及上述附图中的术语“第一”、“第二”等是用于区别类似的对象,而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换,以便这里描述的本发明的实施例能够以除了在这里图示或描述的那些以外的顺序实施。此外,术语“包括”和“具有”以及他们的任何变形,意图在于覆盖不排他的包含,例如,包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元,而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。

[0027] 需要说明的是,本公开所涉及的相关信息(包括但不限于用户设备信息、用户个人信息等)和数据(包括但不限于用于展示的数据、分析的数据等),均为经用户授权或者经过各方充分授权的信息和数据。例如,本系统和相关用户或机构间设置有接口,在获取相关信

息之前,需要通过接口向前述的用户或机构发送获取请求,并在接收到前述的用户或机构反馈的同意信息后,获取相关信息。

#### [0028] 实施例1

[0029] 根据本发明实施例,提供了一种基于区块链的证书管理方法的实施例,需要说明的是,在附图的流程图示出的步骤可以在诸如一组计算机可执行指令的计算机系统中执行,并且,虽然在流程图中示出了逻辑顺序,但是在某些情况下,可以以不同于此处的顺序执行所示出或描述的步骤。

[0030] 在本实施例中,如图1所示,以一种可选的证书管理系统为执行主体执行前述的基于区块链的证书管理方法,该证书管理系统至少包括证书查询模块、证书展示模块以及数字藏品发行系统,还可以包括证书制作模块,其中,数字藏品发行系统可以包括区块链模块、数字藏品技术模块。可选的,可以在慈善机构的相关平台内搭建该证书管理系统。

[0031] 图2是根据本发明实施例的一种可选的证书管理方法的示意图,如图2所示,该方法包括如下步骤:

[0032] 步骤S201,确定目标对象的权限信息,并依据权限信息确定第一目标模块。

[0033] 在步骤S201中,可选的,证书管理系统可以确定目标对象的权限信息,并基于目标对象的权限信息确定目标对象获取证书的权限,从而根据前述的权限确定用于响应目标对象的相关指令的第一目标模块。其中,前述的目标对象为待查询数字捐赠证书的对象,前述的目标对象可以是其所要查询的数字捐赠证书的拥有者,也可以是是需要用到该数字捐赠证书的相关权威机构或金融机构,例如,相关权威机构可以根据该数字捐赠证书为数字捐赠证书的拥有者提供扣税优惠证明或办理相关业务,相关金融机构可以根据该数字捐赠证书为数字捐赠证书的拥有者办理相关业务等,第一目标模块可以是前述的证书查询模块,也可以是前述的证书展示模块。

[0034] 步骤S202,通过第一目标模块响应目标对象的证书查询指令。

[0035] 在步骤S202中,证书管理系统可以通过确定好的第一目标模块响应目标对象的证书查询指令,从而通过第一目标模块基于证书查询指令执行为目标对象查询证书的操作。其中,前述的证书查询指令中至少包括查询信息,查询信息可以是所要查询的数字捐赠证书所对应的捐赠者身份标识、证书哈希值、证书编号等信息,查询信息也可以是其它能够表征所要查询的数字捐赠证书的特征的信息。

[0036] 需要说明的是,通过基于不同的模块响应不同权限的目标对象的指令,便于基于不同的方式反馈目标对象所要查询的数字捐赠证书,从而避免了基于相同的方式向不同的目标对象反馈目标数字捐赠证书造成的可信度低的对象对直接获取的目标数字捐赠证书容易伪造或是可信度高的对象对图片形式的目标数字捐赠证书难以留存的现象。

[0037] 步骤S203,从第二目标模块中确定证书查询指令所要查询的目标数字捐赠证书,其中,第二目标模块用于存储目标数字捐赠证书。

[0038] 在步骤S203中,第一目标模块可以直接从第二目标模块中确定证书查询指令所要查询的目标数字捐赠证书,第一目标模块也可以向其它模块发送控制指令,以控制其它模块从第二目标模块中确定证书查询指令所要查询的目标数字捐赠证书,并从其它模块获取到目标数字捐赠证书,其中,前述的其它模块为证书捐赠系统中除第一目标模块以外的模块,前述的第二目标模块可以是数字藏品技术模块。

[0039] 可选的,在从第二目标模块中确定证书查询指令所要查询的目标数字捐赠证书的过程中,第一目标模块或其它目标模块可以将查询信息的信息内容与第二目标模块中所存储的至少一个数字捐赠证书相匹配,从而将与前述信息内容一致的数字捐赠证书确定为目标数字捐赠证书。

[0040] 需要说明的是,通过在将目标数字捐赠证书存储在第二目标模块中,便于相关用户或机构通过手机、电脑等互联网设备在线查询、浏览和展示,解决了纸质证书不方便携带的困扰,同时,还避免了纸质形式的捐赠证书容易伪造的问题。

[0041] 步骤S204,基于区块链中存储的信息对目标数字捐赠证书进行真实性验证,并在确定目标数字捐赠证书真实的情况下,通过第一目标模块将目标数字捐赠证书以目标方式反馈给目标对象,其中,区块链至少用于存储数字捐赠证书对应的哈希值,第一目标模块与目标方式相对应。

[0042] 在步骤S204中,当第一目标模块获取到目标数字捐赠证书之后,第一目标模块可以先计算所获取到的目标数字捐赠证书的哈希值,然后从区块链(也即前述的区块链模块)中查找与前述的证书查询指令中的查询信息所对应的哈希值,接着,第一目标模块可以将前述计算得到的哈希值与查找到的哈希值进行比对,从而在两哈希值相同时,确定目标数字捐赠证书真实,反之,在两哈希值不同时,确定目标数字捐赠证书异常,从而实现对目标数字捐赠证书的真实性验证。可选的,因实际应用情况的不同,证书查询指令中的查询信息可能包括有目标对象所要查询的证书的哈希值,因此,第一目标模块也可以将从查询信息中获取的哈希值直接与从区块链中查找到的哈希值进行比对,从而验证目标数字捐赠证书的真实性。此外,区块链中也可以存储有至少一个数字捐赠证书所对应的证书信息,并将证书信息直接与目标数字捐赠证书比对,以对目标数字捐赠证书进行真实性验证,其中,前述的证书信息至少包括捐赠信息,还可以包括数字捐赠证书的证书格式。

[0043] 进一步地,当第一目标模块确定目标数字捐赠真实后,第一目标模块可以将目标数字捐赠证书基于目标方式反馈给目标对象,其中,前述的目标方式可以是目标数字捐赠证书直接发送给目标对象,也可以是将目标数字捐赠证书展示给目标对象,还可以是将目标数字捐赠证书进行加密后发送给目标对象,以使得目标对象在对目标数字捐赠证书解密后才能获取到该目标数字捐赠证书。其中,需要强调的是,第一目标模块也可以在控制其它模块获取到目标数字捐赠证书之后,控制其它模块对目标数字捐赠证书进行真实性验证,并在真实性验证通过的情况下,从其它模块处获取该真实的目标数字捐赠证书,以便基于目标方式反馈给目标对象。

[0044] 需要说明的是,由于在区块链透明共享和防篡改的能力支撑下,使得区块链能够有效保证其所存储的信息不可篡改、不可伪造、不可抵赖、可全程留痕,因此,通过将数字捐赠证书的哈希值存储到区块链中,并在将目标对象所查询的目标数字捐赠证书反馈给目标对象之前,基于区块链中的存储的哈希值对第二目标模块中的目标数字捐赠证书进行真实性验证,可以有效保证验证结果的有效性,从而保证发送给目标对象的目标数字捐赠证书的真实性。

[0045] 基于上述步骤S201至步骤S204所限定的方案,可以获知,在本发明实施例中,采用基于区块链中存储的信息对目标对象所要查询的证书进行真实性验证,并在验证成功后将证书反馈给目标对象的方式,通过确定目标对象的权限信息,并依据权限信息确定第一目



标模块,然后通过第一目标模块响应目标对象的证书查询指令,接着从第二目标模块中确定证书查询指令所要查询的目标数字捐赠证书,从而基于区块链中存储的信息对目标数字捐赠证书进行真实性验证,并在确定目标数字捐赠证书真实的情况下,通过第一目标模块将目标数字捐赠证书以目标方式反馈给目标对象。其中,第二目标模块用于存储目标数字捐赠证书,区块链至少用于存储数字捐赠证书对应的哈希值,第一目标模块与目标方式相对应。

[0046] 容易注意到的是,在上述过程中,由于区块链能够有效保证其所存储的信息不可篡改、不可伪造、不可抵赖、可全程留痕,因此,通过将数字捐赠证书的哈希值存储到区块链中,并在将目标对象所查询的目标数字捐赠证书反馈给目标对象之前,基于区块链中的存储的哈希值对第二目标模块中的目标数字捐赠证书进行真实性验证,可以有效保证验证结果的有效性,从而保证了发送给目标对象的目标数字捐赠证书的真实性,避免了现有技术中纸质捐赠证书易伪造的问题。此外,通过基于目标对象权限的不同,采用不同的方式反馈目标对象所要查询的数字捐赠证书,避免了基于相同的方式向不同的目标对象反馈目标数字捐赠证书造成的可信度低的对象对直接获取的目标数字捐赠证书容易伪造或是可信度高的对象对图片形式的目标数字捐赠证书难以留存的现象,从而更进一步地保证了捐赠证书的真实性。

[0047] 由此可见,本申请所提供的方案达到了基于区块链中存储的信息对目标对象所要查询的证书进行真实性验证,并在验证成功后将证书反馈给目标对象的目的,从而实现了提高捐赠证书真实性的技术效果,进而解决了现有技术中由于纸质的捐赠证书易伪造所造成的证书真实性低的技术问题。

[0048] 在一种可选的实施例中,在确定目标对象的权限信息之前,证书管理系统可以获得捐赠对象向目标机构进行捐赠的捐赠信息,然后基于捐赠信息生成数字捐赠证书,并生成与数字捐赠证书对应的哈希值,从而将与数字捐赠证书对应的哈希值以及捐赠信息存储到区块链中。

[0049] 可选的,如图1所示,当社会爱心人士或相关机构向慈善机构(即前述的目标机构)进行慈善捐赠之后,证书管理系统可以响应慈善机构的捐赠信息发送请求,并基于捐赠信息发送请求调用证书制作模块的接口,从而由证书制作模块获取慈善机构发送的捐赠对象向该慈善机构进行捐赠的捐赠信息。进一步地,证书制作模块可以在接收到慈善机构的收到相关指令及信息后,对所获取的捐赠信息进行数据处理,然后将数据处理后的捐赠信息生成数字捐赠证书,并可以将生成的数字捐赠证书或是数字捐赠证书所对应的信息发送给数字藏品技术模块,也即将生成的数字捐赠证书以图片或3D数据格式传递给数字藏品技术模块。其中,前述的捐赠信息可以包括捐赠对象的对象信息、捐赠时间、捐赠金额、受捐对象等信息,前述的数据处理可以是数据清洗、数据标准化等处理方式中的至少之一。

[0050] 进一步地,当数字藏品技术模块获取到数字捐赠证书之后,数字藏品技术模块可以完成捐赠证书数字藏品的铸造和证书关键信息及其哈希值上链存证,以实现将捐赠证书的数字藏品化。具体地,数字藏品技术模块可以提取数字捐赠证书所对应的捐赠对象的对象信息、捐赠日期、捐赠金额、受捐对象等关键信息,并通过加密算法对前述提取出的关键信息进行计算,从而得到与数字捐赠证书对应的哈希值,之后,数字藏品技术模块可以将前述的关键信息与哈希值上传并存储到区块链中,以完成对数字捐赠证书的数字藏品化。其

中,基于区块链的数字藏品是使用区块链技术通过唯一标识确认权益归属的数字作品、艺术品和商品,数字藏品能够在区块链网络中标记出其所有者,并便于对后续的流转进行追溯,数字藏品包括但不限于数字图片、音乐、视频、电子票证、数字纪念品等各种形式。

[0051] 可选的,在本实施例中,如图1所示,区块链模块的主要作用是在链上存储记录数字捐赠证书的相关信息。该区块链模块可根据业务需要选用任何一种区块链底层技术构建区块链网络,且区块链网络各个节点的主体可以包含慈善机构、权威机构、金融机构、监管机构等。其中,慈善机构可以负责运营证书管理系统和区块链模块,以至至少将数字捐赠证书进行上链存储。金融机构可以通过核对本机构内部的转账信息,对数字捐赠证书记载的信息进行共识;权威机构可对区块链上共享的信息进行背书,提供第三方的公信力;监管机构可以访问区块链上共享的信息,对慈善机构每一时期内的款物运作情况进行审计,以对慈善机构进行实时监督。

[0052] 需要说明的是,通过在区块链中引入第三方公证机构进行背书,经过区块链网络中各个节点的共识,使得不同的业务方在从区块链上获取相关信息时,更加便携高效,且相关信息的真实性可以得到进一步地保障,从而减少了多方信息核查和验证的成本及时间,提高了办事效率。此外,数字化的捐赠证书形式,提升了捐赠证书的便携性,区块链数字藏品能力的加持,使得捐赠证书相比于一般的电子版数字证书更加具有可信度,可获得相关机构的认可,极大的推动捐赠证书的使用范围,真正发挥捐赠证书的使用效力,同时便于相关机构进行查询和追溯,进而便于对慈善机构进行透明监管,促进慈善机构更加透明可信管理,提升其社会公信力。

[0053] 在一种可选的实施例中,在基于捐赠信息生成数字捐赠证书的过程中,证书管理系统可以获取捐赠对象发送的目标证书格式,然后基于捐赠信息以及目标证书格式生成数字捐赠证书。

[0054] 可选的,证书制作模块可以在获取捐赠信息时,同时获取捐赠对象发送的目标证书格式,其中,该目标证书格式可以是证书制作模块所内置的多种可选图形或三维展示模式中选择,也可以是捐赠对象所自定义的。之后,证书制作模块可以依据捐赠信息和目标证书格式,按照捐赠对象的个性化审美需求定制生成数字捐赠证书。

[0055] 进一步地,在生成与数字捐赠证书对应的哈希值的过程中,数字藏品技术模块可以在获取数字捐赠证书对应的捐赠对象的对象信息、捐赠日期、捐赠金额、受捐对象的同时,将目标证书格式同样作为关键信息,从而基于捐赠对象的对象信息、捐赠日期、捐赠金额、受捐对象以及目标证书格式生成哈希值。

[0056] 需要说明的是,通过依据捐赠对象的个性化需求将捐赠证书制作成数字藏品,赋予了捐赠证书更多的收藏价值,从而可以提升捐赠对象捐赠的捐赠体验和新奇性,进而推动社会公众对于慈善事业的关注度。

[0057] 在一种可选的实施例中,在基于区块链中存储的信息对目标数字捐赠证书进行真实性验证的过程中,证书管理系统可以计算与目标数字捐赠证书对应的哈希值,然后从区块链中确定与证书查询指令中的查询信息对应的第一目标哈希值,从而在目标数字捐赠证书对应的哈希值与第一目标哈希值相同的情况下,确定目标数字捐赠证书真实,在目标数字捐赠证书对应的哈希值与第一目标哈希值不同的情况下,确定目标数字捐赠证书异常。

[0058] 可选的,第一目标模块可以基于所获取到的目标数字捐赠证书对应的捐赠信息先

计算所获取到的目标数字捐赠证书的哈希值,第一目标模块也可以基于所获取到的目标数字捐赠证书对应的捐赠信息以及目标证书格式计算所获取到的目标数字捐赠证书的哈希值。之后,第一目标模块可以从区块链中查找与前述的证书查询指令中的查询信息所对应的哈希值(也即第一目标哈希值),从而在两哈希值相同时,确定目标数字捐赠证书真实,反之,在两哈希值不同时,确定目标数字捐赠证书异常。

[0059] 需要说明的是,通过将目标数字捐赠证书对应的哈希值与区块链中存储的哈希值进行比对,实现了对目标数字捐赠证书真实性的有效验证。

[0060] 在一种可选的实施例中,在确定目标对象的权限信息,并依据权限信息确定第一目标模块的过程中,若目标对象的权限信息为第一权限信息,则确定目标对象为第一目标对象,并将证书查询模块确定为第一目标模块,若目标对象的权限信息为第二权限信息,则确定目标对象为第二目标对象,并将证书展示模块确定为第一目标模块,其中,第一权限信息所表征的权限高于第二权限信息所表征的权限。

[0061] 在本实施例中,可以预先将相关权威机构等权威用户的权限信息设置为第一权限信息,将个人或金融机构等非权威用户的权限信息设置为第二权限信息。

[0062] 可选的,证书查询模块用于为权威用户(如:外部权威机构)提供捐赠证书的查询功能,即若目标对象的权限信息为第一权限信息,则将证书查询模块确定为第一目标模块。例如,如图1所示,当捐赠对象在办理某项业务(如:扣税优惠证明)时,外部权威机构(即前述的第一目标对象)需要同步捐赠对象的捐赠证书信息,因此,外部权威机构可以与证书查询模块进行系统对接,证书查询模块可以依据该外部权威机构提供的查询信息中的捐赠者身份标识或者证书哈希值等关键字,从数字藏品技术模块获取目标数字捐赠证书并对目标数字捐赠证书进行真实性验证。

[0063] 可选的,证书展示模块用于为非权威用户(如:捐赠对象、相关金融机构)提供捐赠证书的查询功能,即若目标对象的权限信息为第二权限信息,则将证书展示模块确定为第一目标模块。例如,如图1所示,当捐赠对象(即前述的第二目标对象)或其他查询方(即前述的第二目标对象)需要查询或浏览数字捐赠证书时,证书展示模块可依据该查询方提供的查询信息中的捐赠者身份标识或者证书编号信息等关键字,通过证书查询模块从数字藏品技术模块获取目标数字捐赠证书,并通过证书展示模块或证书查询模块对目标数字捐赠证书进行真实性验证。

[0064] 需要说明的是,由于第一目标模块与反馈的目标方式相对应,因此,通过在目标对象权限较高时,基于证书查询模块响应目标对象,在目标对象权限较低时,基于证书展示模块响应目标对象,以便于实现对不同目标对象所对应的目标方式的准确选择。

[0065] 在一种可选的实施例中,在通过第一目标模块将目标数字捐赠证书以目标方式反馈给目标对象的过程中,当第一目标模块为证书查询模块时,证书管理系统可以将目标数字捐赠证书发送给第一目标对象,当第一目标模块为证书展示模块,证书管理系统可以向第二目标对象展示目标数字捐赠证书。

[0066] 可选的,当第一目标模块为证书查询模块时,如图1所示,证书查询模块可以将目标数字捐赠证书直接发送给第一目标对象,以便于第一目标对象对数字捐赠证书进行备份、存储等操作,当第一目标模块为证书展示模块时,证书展示模块可以避免将目标数字捐赠证书直接发送给第二目标对象,而是将目标数字捐赠证书转换为图片或文字的形式,然

后通过第二目标对象所持有的手机等终端设备进行真实的证书信息展示。

[0067] 需要说明的是,通过基于不同的方式反馈目标对象所要查询的数字捐赠证书,从而避免了基于相同的方式向不同的目标对象反馈目标数字捐赠证书造成的可信度低的目标对象对直接获取的目标数字捐赠证书容易伪造或是可信度高的目标对象对图片形式的目标数字捐赠证书难以留存的现象。

[0068] 在一种可选的实施例中,在向第二目标对象展示目标数字捐赠证书之后,证书管理系统可以响应第三目标对象的目标证书查询指令,并基于目标证书查询指令确定目标查询信息,然后从区块链中确定与目标标识对应的第三目标哈希值,从而比对第二目标哈希值与第三目标哈希值是否相同,并将比对结果反馈给第三目标对象,其中,第三目标对象用于为第二目标对象办理待办业务,目标查询信息至少包括第二目标对象所提供的目标标识以及第二目标哈希值,比对结果用于第三目标对象确定是否为第二目标对象办理待办业务。

[0069] 可选的,当捐赠对象在相关金融机构(即前述的第三目标对象)办理待办业务时,若捐赠对象需要向相关金融机构展示其数字捐赠证书,则相关金融机构可以在查看到捐赠对象所展示的数字捐赠证书之后,可以基于捐赠对象所展示的数字捐赠证书,确定与被展示的数字捐赠证书对应的目标标识(如:捐赠者身份标识、证书编号等)以及第二目标哈希值,然后向证书管理系统发送对应的目标证书查询指令以进行信息核查。之后,可以通过证书展示模块从该目标证书查询指令中确定目标标识以及第二目标哈希值,并从区块链中查找到与目标标识对应的第三目标哈希值,从而将第二目标哈希值与第三目标哈希值进行比对,得到比对结果,并发送给相关金融机构。其中,相关金融机构可以访问证书管理系统对外开放的证书查询网站,以实现对相关数字捐赠证书的查询。

[0070] 可选的,如图1所示,若在区块链中存在有与前述的第三目标对象所对应的节点,则第三目标对象也可以直接与区块链进行信息交互,以获取与目标标识对应的第三目标哈希值,从而实现对捐赠对象所展示的数字捐赠证书的信息核查。

[0071] 进一步地,当相关金融机构确定第二目标哈希值与第三目标哈希值相同时,其可以选择为该捐赠对象办理待办业务,反之,其可以拒绝为该捐赠对象办理待办业务。

[0072] 需要说明的是,通过基于第三目标对象的目标证书查询指令,为其反馈证书哈希值比对结果,提高了本申请的适用性,并便于扩大捐赠证书的应用范围。

[0073] 可选的,如图3所示,对本申请的一种可选的应用过程进行说明。可选的,对捐赠证书进行数字藏品化的过程可以包括如下步骤:

[0074] 1、捐赠对象或被捐赠对象捐赠的慈善机构调用证书制作模块接口,将捐赠信息传递给证书制作模块。

[0075] 2、证书制作模块基于捐赠信息生成对应的数字捐赠证书,并将数字捐赠证书传递给数字藏品技术模块进行数字藏品铸造。

[0076] 3、数字藏品技术模块调用区块链存证智能合约,将数字捐赠证书的关键信息(如:捐赠信息、证书格式等)以及哈希值进行上链存证。

[0077] 进一步地,如图3所示,当查询方为外部权威机构时,对数字捐赠证书进行查询及反馈的过程可以包括如下步骤:

[0078] 4、外部权威机构访问证书查询模块,并发送证书查询指令以查询证书信息。

[0079] 5、证书查询模块访问数字藏品技术模块,依据证书查询指令中的查询信息查询对应的数字捐赠证书。

[0080] 6、数字藏品技术模块依据证书查询模块发送的信息,反馈对应的数字捐赠证书给证书查询模块。

[0081] 7、证书查询模块对数字捐赠证书进行真实性验证,并在验证通过后将数字捐赠证书发送给外部权威机构。

[0082] 可选的,如图3所示,当查询方为捐赠对象或其它相关机构时,对数字捐赠证书进行查询及反馈的过程可以包括如下步骤:

[0083] 8、捐赠对象(或其它相关机构)访问证书展示模块,并发送证书查询指令以申请浏览证书信息。

[0084] 9、证书展示模块访问证书查询模块,并申请查询证书信息。

[0085] 10、证书查询模块访问数字藏品技术模块,查询对应的数字捐赠证书,并对获取的数字捐赠证书进行真实性验证,然后在验证通过后将数字捐赠证书反馈给证书展示模块。

[0086] 11、证书展示模块将数字捐赠证书展示给捐赠对象(或其它相关机构)。

[0087] 12、为捐赠对象办理待办业务的相关金融机构(也即图3中的查询方)可以通过证书展示模块,调用区块链查询合约,基于从捐赠对象处获取的证书标号或捐赠者身份标识,以及哈希值,查询链上存储的证书信息与哈希值,并由区块链通过证书展示模块将查询到的信息反馈给相关金融机构。可选的,证书展示模块也可以直接对两哈希值进行比对,并将带有比对结果的相关信息反馈给相关金融机构。

[0088] 由此可见,本申请所提供的方案达到了基于区块链中存储的信息对目标对象所要查询的证书进行真实性验证,并在验证成功后将证书反馈给目标对象的目的,从而实现了提高捐赠证书真实性的技术效果,进而解决了现有技术中由于纸质的捐赠证书易伪造所造成的证书真实性低的技术问题。

[0089] 实施例2

[0090] 根据本发明实施例,提供了一种基于区块链的证书管理装置的实施例,其中,图4是根据本发明实施例的一种可选的证书管理装置的示意图,如图4所示,该装置包括:

[0091] 第一确定模块401,用于确定目标对象的权限信息,并依据权限信息确定第一目标模块;

[0092] 响应模块402,用于通过第一目标模块响应目标对象的证书查询指令;

[0093] 第二确定模块403,用于从第二目标模块中确定证书查询指令所要查询的目标数字捐赠证书,其中,第二目标模块用于存储目标数字捐赠证书;

[0094] 反馈模块404,用于基于区块链中存储的信息对目标数字捐赠证书进行真实性验证,并在确定目标数字捐赠证书真实的情况下,通过第一目标模块将目标数字捐赠证书以目标方式反馈给目标对象,其中,区块链至少用于存储数字捐赠证书对应的哈希值,第一目标模块与目标方式相对应。

[0095] 需要说明的是,上述第一确定模块401、响应模块402、第二确定模块403以及反馈模块404对应于上述实施例中的步骤S201至步骤S204,四个模块与对应的步骤所实现的示例和应用场景相同,但不限于上述实施例1所公开的内容。

[0096] 可选的,基于区块链的证书管理装置还包括:第一获取模块,用于获取捐赠对象向

目标机构进行捐赠的捐赠信息;生成模块,用于基于捐赠信息生成数字捐赠证书,并生成与数字捐赠证书对应的哈希值;存储模块,用于将与数字捐赠证书对应的哈希值以及捐赠信息存储到区块链中。

[0097] 可选的,生成模块还包括:第二获取模块,用于获取捐赠对象发送的目标证书格式;生成子模块,用于基于捐赠信息以及目标证书格式生成数字捐赠证书。

[0098] 可选的,反馈模块还包括:计算模块,用于计算与目标数字捐赠证书对应的哈希值;第一确定子模块,用于从区块链中确定与证书查询指令中的查询信息对应的第一目标哈希值;第二确定子模块,用于在目标数字捐赠证书对应的哈希值与第一目标哈希值相同的情况下,确定目标数字捐赠证书真实;第三确定子模块,用于在目标数字捐赠证书对应的哈希值与第一目标哈希值不同的情况下,确定目标数字捐赠证书异常。

[0099] 可选的,第一确定模块还包括:第四确定子模块,用于若目标对象的权限信息为第一权限信息,则确定目标对象为第一目标对象,并将证书查询模块确定为第一目标模块;第五确定子模块,用于若目标对象的权限信息为第二权限信息,则确定目标对象为第二目标对象,并将证书展示模块确定为第一目标模块,其中,第一权限信息所表征的权限高于第二权限信息所表征的权限。

[0100] 可选的,反馈模块还包括:发送模块,用于当第一目标模块为证书查询模块时,将目标数字捐赠证书发送给第一目标对象;展示模块,用于当第一目标模块为证书展示模块,向第二目标对象展示目标数字捐赠证书。

[0101] 可选的,基于区块链的证书管理装置还包括:第六确定子模块,用于响应第三目标对象的目标证书查询指令,并基于目标证书查询指令确定目标查询信息,其中,第三目标对象用于为第二目标对象办理待办业务,目标查询信息至少包括第二目标对象所提供的目标标识以及第二目标哈希值;第七确定子模块,用于从区块链中确定与目标标识对应的第三目标哈希值;比对模块,用于比对第二目标哈希值与第三目标哈希值是否相同,并将比对结果反馈给第三目标对象,其中,比对结果用于第三目标对象确定是否为第二目标对象办理待办业务。

[0102] 实施例3

[0103] 根据本发明实施例的另一方面,还提供了计算机可读存储介质,计算机可读存储介质中存储有计算机程序,其中,计算机程序被设置为运行时执行上述的基于区块链的证书管理方法。

[0104] 实施例4

[0105] 根据本发明实施例的另一方面,还提供了一种电子设备,其中,图5是根据本发明实施例的一种可选的电子设备的示意图,如图5所示,电子设备包括一个或多个处理器;存储器,用于存储一个或多个程序,当一个或多个程序被一个或多个处理器执行时,使得一个或多个处理器实现用于运行程序,其中,程序被设置为运行时执行上述的基于区块链的证书管理方法。

[0106] 上述本发明实施例序号仅仅为了描述,不代表实施例的优劣。

[0107] 在本发明的上述实施例中,对各个实施例的描述都各有侧重,某个实施例中沒有详述的部分,可以参见其他实施例的相关描述。

[0108] 在本申请所提供的几个实施例中,应该理解到,所揭露的技术内容,可通过其它的

方式实现。其中,以上所描述的装置实施例仅仅是示意性的,例如单元的划分,可以为一种逻辑功能划分,实际实现时可以有另外的划分方式,例如多个单元或组件可以结合或者可以集成到另一个系统,或一些特征可以忽略,或不执行。另一点,所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口,单元或模块的间接耦合或通信连接,可以是电性或其它的形式。

[0109] 作为分离部件说明的单元可以是或者也可以不是物理上分开的,作为单元显示的部件可以是或者也可以不是物理单元,即可以位于一个地方,或者也可以分布到多个单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0110] 另外,在本发明各个实施例中的各功能单元可以集成在一个处理单元中,也可以是各个单元单独物理存在,也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现,也可以采用软件功能单元的形式实现。

[0111] 集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用,可以存储在一个计算机可读取存储介质中。基于这样的理解,本发明的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式体现出来,该计算机软件产品存储在一个存储介质中,包括若干指令用以使得一台计算机设备(可为个人计算机、服务器或者网络设备等)执行本发明各个实施例方法的全部或部分步骤。而前述的存储介质包括:U盘、只读存储器(ROM,Read-Only Memory)、随机存取存储器(RAM,Random Access Memory)、移动硬盘、磁碟或者光盘等各种可以存储程序代码的介质。

[0112] 以上仅是本发明的优选实施方式,应当指出,对于本技术领域的普通技术人员来说,在不脱离本发明原理的前提下,还可以做出若干改进和润饰,这些改进和润饰也应视为本发明的保护范围。

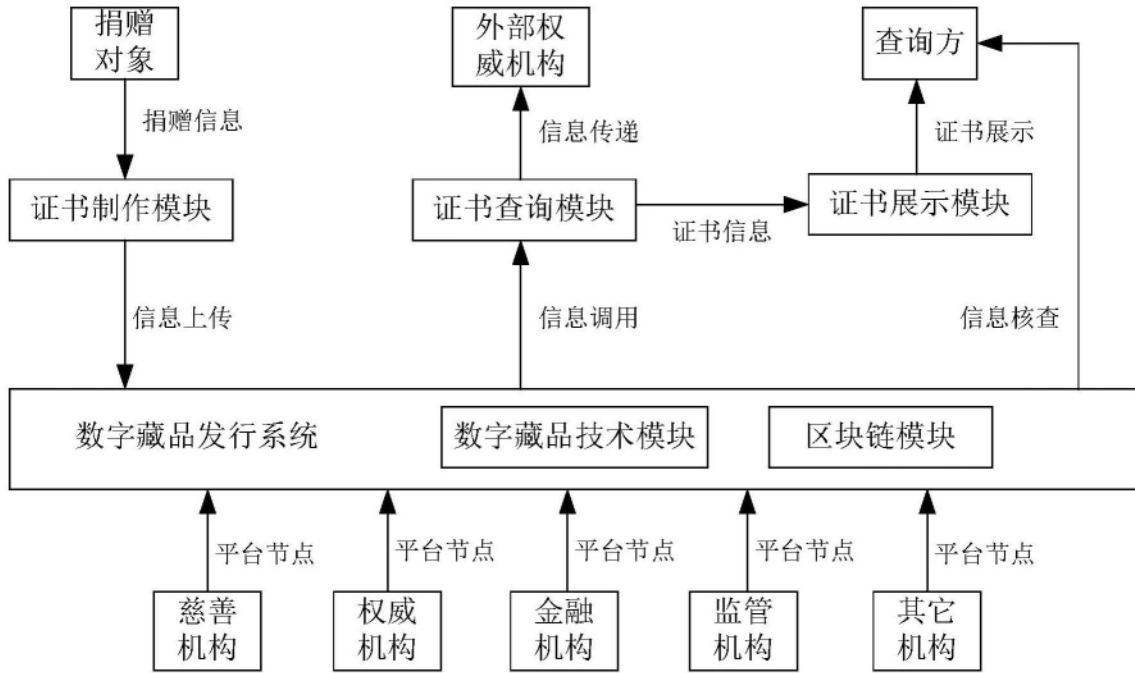


图1

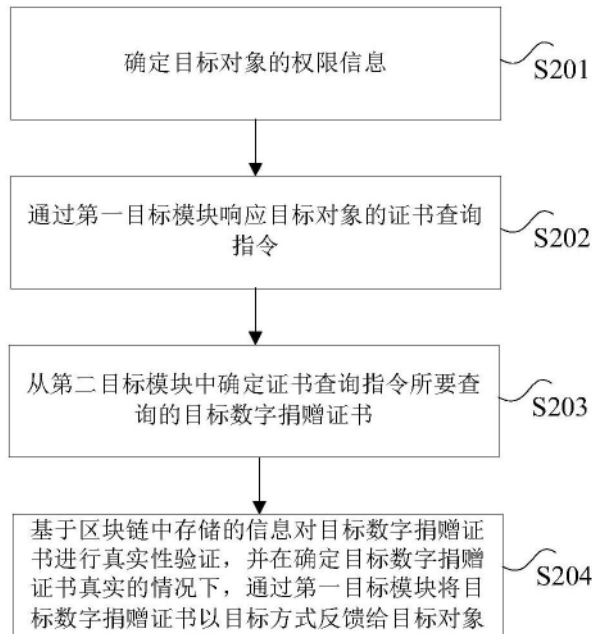


图2



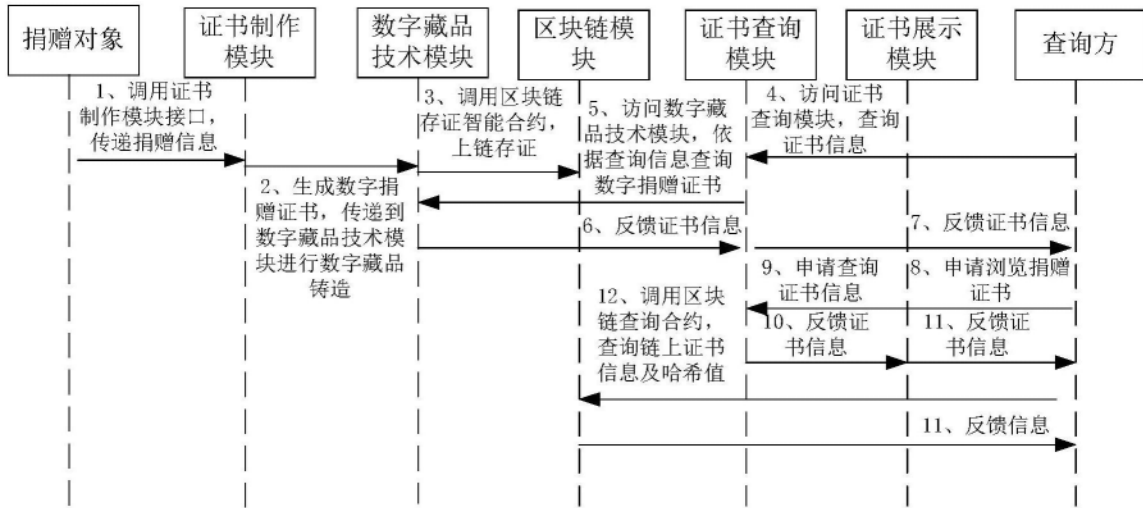


图3



图4

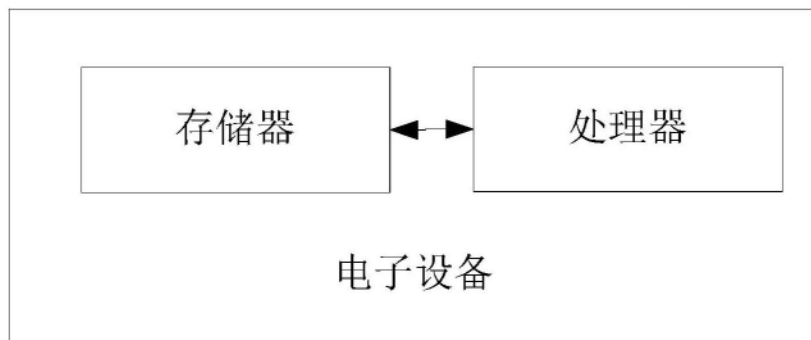


图5