(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 112100178 A
(43)申请公布日 2020.12.18

(21)申请号 202010937142.6

(22)申请日 2020.09.08

(71)申请人 中国联合网络通信集团有限公司
地址 100033 北京市西城区金融大街21号

(72)发明人 张伦泳

(74)专利代理机构 北京天昊联合知识产权代理有限公司 11112
代理人 彭瑞欣 刘悦晗

(51)Int.Cl.
G06F 16/22(2019.01)
G06F 16/27(2019.01)
G06F 21/64(2013.01)
G06Q 50/16(2012.01)

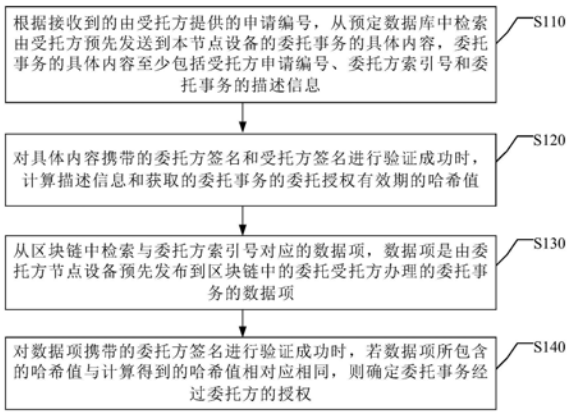
权利要求书3页 说明书11页 附图6页

(54)发明名称

委托授权验证方法和系统

(57)摘要

本申请公开了一种委托授权验证方法和系统，该方法包括：根据接收到受托方提供的申请编号，检索由受托方预先发送的委托事务的具体内容；对具体内容携带的委托方签名和受托方签名进行验证成功时，计算描述信息和获取的委托事务的委托授权有效期的哈希值；从区块链中检索与委托方索引号对应的数据项，数据项是由委托方节点设备预先发布到区块链中的委托受托方办理的委托事务的数据项；对数据项携带的委托方签名进行验证成功时，若数据项所包含的哈希值与计算得到的哈希值相对应相同，则确定委托事务经过委托方的授权。根据本申请实施例提供的方法，确保委托人的利益免受不正当的损害。



CN 112100178 A

1.一种委托授权验证方法,其特征在于,应用于执行方节点设备,包括:

根据接收到的由受托方提供的申请编号,从预定数据库中检索由所述受托方预先发送到本节点设备的委托事务的具体内容,所述委托事务的具体内容至少包括受托方申请编号、委托方索引号和所述委托事务的描述信息;

对所述具体内容携带的委托方签名和受托方签名进行验证成功时,计算所述描述信息和获取的所述委托事务的委托授权有效期的哈希值;

从区块链中检索与所述委托方索引号对应的数据项,所述数据项是由委托方节点设备预先发布到区块链中的委托所述受托方办理的委托事务的数据项;

对所述数据项携带的委托方签名进行验证成功时,若所述数据项所包含的哈希值与计算得到的哈希值相对应相同,则确定所述委托事务经过委托方的授权。

2.根据权利要求1所述的方法,其特征在于,所述具体内容携带的委托方签名和受托方签名包括第一签名、第二签名和第三签名;其中,

所述第一签名是在委托方节点设备,将所述委托方索引号、所述描述信息和所述委托事务的委托授权有效期作为一个整体进行的签名;

所述第二签名是在受托方节点设备,对所述受托方申请编号进行的签名,所述第三签名是在受托方节点设备,将所述委托方索引号、所述描述信息和所述委托授权有效期作为一个整体进行的签名;

所述对所述具体内容携带的委托方签名和受托方签名进行验证,包括:

根据所述受托方预先在区块链中完成的实名认证信息,验证所述第二签名和所述第三签名;根据所述委托方预先在区块链中完成的实名认证信息,验证所述第一签名。

3.根据权利要求2所述的方法,其特征在于,若所述委托事务的具体内容附带至少一个电子文件,则所述具体内容携带的委托方签名和受托方签名还包括第四签名和第五签名;其中,

所述第四签名包括在委托方节点设备对所述附带的每个电子文件进行的签名,所述第五签名包括在受托方节点设备,对所述附带的每个电子文件进行的签名;

所述对所述具体内容携带的委托方签名和受托方签名进行验证,还包括:

根据所述受托方预先在区块链中完成的实名认证信息,验证所述第五签名;根据所述委托方预先在区块链中完成的实名认证信息,验证所述第四签名。

4.根据权利要求1所述的方法,其特征在于,若所述委托事务的具体内容未附带电子文件,则所述数据项携带的委托方签名为第六签名,所述第六签名是在委托方节点设备,将所述委托方索引号和第一哈希值作为一个整体进行的签名;其中,

所述第一哈希值是在委托方节点设备,将所述委托授权有效期和所述描述信息作为一个整体计算得到的哈希值;

所述对所述数据项携带的委托方签名进行验证成功时,若所述数据项所包含的哈希值与计算得到的哈希值相对应相同,则确定所述委托事务经过委托方的授权,包括:

若验证所述第六签名成功,对所述委托授权有效期和所述描述信息进行哈希计算得到的哈希值与所述第一哈希值相同,且当前日期在所述委托授权有效期内,则确定所述委托事务经过委托方的授权。

5.根据权利要求4所述的方法,其特征在于,若所述委托事务的具体内容附带至少一个

电子文件，则所述数据项携带的委托方签名为第七签名，所述第七签名是在委托方节点设备，将所述委托方索引号、所述第一哈希值和计算得到的第二哈希值作为一个整体进行的签名；其中，

所述第二哈希值是分别对附带的每个电子文件进行计算得到的所述每个电子文件的哈希值；

所述对所述数据项携带的委托方签名进行验证成功时，若所述数据项所包含的哈希值与计算得到的哈希值相对应相同，则确定所述委托事务经过委托方的授权，包括：

若验证所述第七签名成功，对所述委托授权有效期和所述描述信息进行哈希计算得到的哈希值与所述第一哈希值相同，对附带的每个电子文件计算的哈希值与所述第二哈希值对应相同，且当前日期在所述委托授权有效期内，则确定所述委托事务经过委托方的授权。

6.根据权利要求1至5中任一项所述的方法，其特征在于，在对所述具体内容携带的委托方签名和受托方签名进行验证之前，所述方法还包括：

若检索到的所述具体内容包含所述委托授权有效期，则确定所述委托事务的委托授权有效期为所述检索到委托授权有效期；

若检索到的所述具体内容未包含所述委托授权有效期，且所述委托事务具有法定有效期，则确定所述委托事务的委托授权有效期为所述法定有效期；

若检索到的所述具体内容未包含所述委托授权有效期，且所述委托事务未具有法定有效期，则确定所述委托事务的委托授权有效期为永久有效期。

7.一种委托授权验证方法，其特征在于，包括：

基于生成的委托事务的描述信息和所述委托事务的委托授权有效期，计算得到第一哈希值；

为所述委托事务分配委托方索引号，对包含所述委托方索引号和所述第一哈希值的数据项进行委托方签名，并将所述委托方签名后的数据项发布到区块链中；

根据所述委托方索引号、所述描述信息和所述委托授权有效期，得到所述委托事务的具体内容，对所述具体内容进行委托方签名，得到委托方签名后的具体内容；

将所述委托方签名后的具体内容通过预定文件形式发送至受托方节点，其中，

所述委托方签名后的具体内容，用于在受托方节点进行受托方签名后被发送至执行方节点，并且所述具体内容在所述执行方节点被用于与所述发布到区块链中的数据项进行哈希值的比对，以确定所述委托事务经过委托方的授权。

8.根据权利要求7所述的方法，其特征在于，若所述委托事务的具体内容附带至少一个电子文件，则所述方法还包括：

分别计算附带的每个电子文件的哈希值，得到第二哈希值，所述第二哈希值中包含所述每个电子文件的哈希值；

所述对包含所述委托方索引号和所述第一哈希值的数据项进行委托方签名，并将所述委托方签名后的数据项发布到区块链中，包括：

对包含所述委托方索引号、所述第一哈希值和所述第二哈希值的数据项进行委托方签名，经将所述委托方签名后的数据项发布到区块链中；

所述根据所述委托方索引号、所述描述信息和所述委托授权有效期，得到所述委托事务的具体内容，对所述具体内容进行委托方签名，得到委托方签名后的具体内容，包括：

将所述委托方索引号、所述描述信息和所述委托授权有效期的委托事务的具体内容作为一个整体进行委托方签名，并对附带的每个电子文件进行委托方签名，得到委托方签名后的具体内容。

9.根据权利要求7所述的方法，其特征在于，若所述委托事务的具体内容附带至少一个电子文件，则所述委托方签名后的具体内容在受托方节点的签名包括如下签名项：

在受托方节点为接收到的所述具体内容分配受托方申请编号后，并对所述申请编号进行的受托方签名；

将所述具体内容中的所述委托方索引号、所述描述信息和所述委托授权有效期作为一个整体进行的受托方签名；

以及，对附带的每个电子文件分别进行的受托方签名。

10.一种委托授权验证系统，包括存储器和处理器；

所述存储器用于储存有可执行程序代码；

所述处理器用于读取所述存储器中存储的可执行程序代码以执行权利要求1至6中任一项、或者权利要求7至9中任一项所述的委托授权验证方法。

委托授权验证方法和系统

技术领域

[0001] 本申请涉及区块链技术领域，具体涉及一种委托授权验证方法和系统。

背景技术

[0002] 日常生活中，经常出现委托他人办理各种日常事务的情况。例如甲委托乙代为签署合同，代为办理银行存取款、理财业务，代为办理房屋过户手续、代为办理公司开办手续等等。但往往由于执行业务操作的执行方，例如合同相对人、银行、房地产管理中心、工商局等，常常无法准确核实受托人的受托权限，无法确定委托方是否真的委托受托方办理具体业务，若出现无权代理的情况，则会导致委托人遭受损失。

[0003] 因此，需要在业务操作执行方实际办理业务操作之前，对受托人的受托权限进行验证，以确保委托人的利益免受不正当损害。

发明内容

[0004] 为此，本申请提供一种委托授权验证方法和系统，以解决现有技术中由于无法准确核实受托人的受托权限而导致的委托人的利益受到不正当损害的问题。

[0005] 为了实现上述目的，本申请第一方面提供一种委托授权验证方法，包括：根据接收到的由受托方提供的申请编号，从预定数据库中检索由受托方预先发送到本节点设备的委托事务的具体内容，委托事务的具体内容至少包括受托方申请编号、委托方索引号和委托事务的描述信息；对具体内容携带的委托方签名和受托方签名进行验证成功时，计算描述信息和获取的委托事务的委托授权有效期的哈希值；从区块链中检索与委托方索引号对应的数据项，数据项是由委托方节点设备预先发布到区块链中的委托受托方办理的委托事务的数据项；对数据项携带的委托方签名进行验证成功时，若数据项所包含的哈希值与计算得到的哈希值相对应相同，则确定委托事务经过委托方的授权。

[0006] 本申请第二方面提供一种委托授权验证方法，包括：基于生成的委托事务的描述信息和委托事务的委托授权有效期，计算得到第一哈希值；为委托事务分配委托方索引号，对包含委托方索引号和第一哈希值的数据项进行委托方签名，并将委托方签名后的数据项发布到区块链中；根据委托方索引号、描述信息和委托授权有效期，得到委托事务的具体内容，对具体内容进行委托方签名，得到委托方签名后的具体内容；将委托方签名后的具体内容通过预定文件形式发送至受托方节点，其中，委托方签名后的具体内容，用于在受托方节点进行受托方签名后被发送至执行方节点，并且具体内容在执行方节点被用于与发布到区块链中的数据项进行哈希值的比对，以确定委托事务经过委托方的授权。

[0007] 本申请第三方面提供一种委托授权验证系统，包括：一个或多个处理器；存储器，其上存储有一个或多个程序，当一个或多个程序被一个或多个处理器执行，使得一个或多个处理器实现本申请实施例中的任意一种方法。

[0008] 本申请具有如下优点：根据本申请实施例中第一方面的委托授权验证方法和执行第一方面中委托授权验证方法的委托授权验证系统，执行方节点设备在实际执行委托事务

之前，可以计算从受托方收到的内容的哈希值，并将此哈希值与从区块链上检索到的带有委托方签名的哈希值进行比较，根据比较结果确定受托方是否真正得到委托方的委托，确保委托人的利益免受不正当的损害；

[0009] 根据本申请实施例中第二方面的委托授权验证方法和执行第二方面中委托授权验证方法的委托授权验证系统，委托方节点设备将委托受托方办理业务的事项，进行签名后发布到区块链中，并将该委托受托方办理业务的事项，进行签名后直接发送给受托方，以进行后续受托方节点和执行方节点的相应处理，确保委托人的利益免受不正当的损害。

附图说明

[0010] 附图是用来提供对本申请的进一步理解，并且构成说明书的一部分，与下面的具体实施方式一起用于解释本申请，但并不构成对本申请的限制。

[0011] 图1是示出根据本申请一实施例的委托授权验证方法的流程图；

[0012] 图2示出本申请另一实施例的委托授权验证方法的流程图；

[0013] 图3示出本申请示例性实施例中应用于委托方节点的委托授权验证的相关处理流程示意图；

[0014] 图4示出本申请示例性实施例中应用于受托方节点的委托授权验证的相关处理流程示意图；

[0015] 图5示出本申请示例性实施例中执行方节点的处理流程示意图；

[0016] 图6示出了根据本申请一实施例提供的委托授权验证装置的结构示意图；

[0017] 图7示出了根据本申请另一实施例提供的委托授权验证装置的结构示意图；

[0018] 图8是示出能够实现根据本申请实施例的委托授权验证方法和装置的计算设备的示例性硬件架构的结构图。

具体实施方式

[0019] 以下结合附图对本申请的具体实施方式进行详细说明。应当理解的是，此处所描述的具体实施方式仅用于说明和解释本申请，并不用于限制本申请。对于本领域技术人员来说，本申请可以在不需要这些具体细节中的一些细节的情况下实施。下面对实施例的描述仅仅是为了通过示出本申请的示例来提供对本申请更好的理解。

[0020] 需要说明的是，在本文中，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、物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、物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……”限定的要素，并不排除在包括要素的过程、方法、物品或者设备中还存在另外的相同要素。

[0021] 为了更好的理解本申请，下面将结合附图，详细描述根据本申请实施例的委托授权验证方法和系统，应注意，这些实施例并不是用来限制本申请公开的范围。

[0022] 图1是示出根据本申请一实施例的委托授权验证方法的流程图。如图1所示，本申请实施例中的委托授权验证方法可以应用于执行方节点设备，并包括以下步骤。

[0023] S110，根据接收到的由受托方提供的申请编号，从预定数据库中检索由受托方预先发送到本节点设备的委托事务的具体内容，委托事务的具体内容至少包括受托方申请编

号、委托方索引号和委托事务的描述信息。

[0024] S120,对具体内容携带的委托方签名和受托方签名进行验证成功时,计算描述信息和获取的委托事务的委托授权有效期的哈希值。

[0025] S130,从区块链中检索与委托方索引号对应的数据项,数据项是由委托方节点设备预先发布到区块链中的委托受托方办理的委托事务的数据项。

[0026] S140,对数据项携带的委托方签名进行验证成功时,若数据项所包含的哈希值与计算得到的哈希值相对应相同,则确定委托事务经过委托方的授权。

[0027] 在本申请实施例中,发布到区块链上的内容采用哈希值,可以使得所发布的内容可验证且不泄露隐私。

[0028] 根据本申请实施例的委托授权验证方法,执行方节点设备在实际执行委托事务之前,可以计算从受托方收到的内容的哈希值,并将此哈希值与从区块链上检索到的带有委托方签名的哈希值进行比较,根据比较结果确定受托方是否真正得到委托方的委托,确保委托人的利益免受不正当的损害。

[0029] 在本申请实施例中,委托事务的具体内容可以包括委托方身份说明信息、受托方身份说明信息和委托事项的具体描述。在一些实施例中,委托事务的具体内容还可以一个或多个附带电子文件,该电子文件可以包括如下电子形式的文件项中的一项或多项:文档、图片和视频。

[0030] 在一个实施例中,具体内容携带的委托方签名和受托方签名包括第一签名、第二签名和第三签名;其中,第一签名是在委托方节点设备,将委托方索引号、描述信息和委托事务的委托授权有效期作为一个整体进行的签名;第二签名是在受托方节点设备对受托方申请编号进行的签名,第三签名是在受托方节点设备,将委托方索引号、描述信息和委托授权有效期作为一个整体进行的签名。

[0031] 步骤S120中,对具体内容携带的委托方签名和受托方签名进行验证的步骤,具体可以包括:S11,根据受托方预先在区块链中完成的实名认证信息,验证第二签名和第三签名;根据委托方预先在区块链中完成的实名认证信息,验证第一签名。

[0032] 在该实施例中,根据受托方预先在区块链中完成的实名认证信息,对在受托方节点设备单独进行签名的受托方申请编号,以及在受托方节点设备将委托方索引号、描述信息和委托授权有效期作为一个整体而进行的签名进行验证。

[0033] 在一个实施例中,若委托事务的具体内容附带至少一个电子文件,则具体内容携带的委托方签名和受托方签名还包括第四签名和第五签名;第四签名包括在委托方节点设备对附带的每个电子文件进行的签名,第五签名包括在受托方节点设备,对附带的每个电子文件进行的签名。

[0034] 步骤S120中对具体内容携带的委托方签名和受托方签名进行验证的步骤,还可以包括:S12,根据受托方预先在区块链中完成的实名认证信息,验证第五签名;根据委托方预先在区块链中完成的实名认证信息,验证第四签名。

[0035] 在该实施例中,若委托事务的具体内容附带电子文件,则对附带的每个电子文件进行单独验证。

[0036] 在一个实施例中,若委托事务的具体内容未附带电子文件,则数据项携带的委托方签名为第六签名,第六签名是在委托方节点设备,将委托方索引号和第一哈希值作为一

个整体进行的签名。其中，第一哈希值是在委托方节点设备，将委托授权有效期和描述信息作为一个整体计算得到的哈希值。

[0037] 上述步骤S140具体可以包括：S21，若验证第六签名成功，对委托授权有效期和描述信息进行哈希计算得到的哈希值与第一哈希值相同，且当前日期在委托授权有效期内，则确定委托事务经过委托方的授权。

[0038] 在该实施例中，若委托事务的具体内容未附带电子文件，则对委托方索引号携带的委托方签名进行验证，以及对将委托授权有效期和委托事务的描述信息作为一个整体携带的委托方签名进行验证，以确定委托事务经过委托方的授权。

[0039] 在一个实施例中，若委托事务的具体内容附带至少一个电子文件，则数据项携带的委托方签名为第七签名，第七签名是在委托方节点设备，将委托方索引号、第一哈希值和计算得到的第二哈希值作为一个整体进行的签名；其中，第二哈希值是分别对附带的每个电子文件进行计算得到的每个电子文件的哈希值。

[0040] 上述步骤S140还可以包括：S22，若验证第七签名成功，对委托授权有效期和描述信息进行哈希计算得到的哈希值与第一哈希值相同，对附带的每个电子文件计算的哈希值与第二哈希值对应相同，且当前日期在委托授权有效期内，则确定委托事务经过委托方的授权。

[0041] 在该实施例中，若委托事务的具体内容附带电子文件，则需要对每个电子文件携带的委托方签名进行验证。

[0042] 在一个实施例中，在步骤S120中之前，该委托授权验证方法还包括如下步骤。

[0043] S31，若检索到的具体内容包含委托授权有效期，则确定委托事务的委托授权有效期为检索到委托授权有效期。

[0044] S32，若检索到的具体内容未包含委托授权有效期，且委托事务具有法定有效期，则确定委托事务的委托授权有效期为法定有效期。

[0045] S33，若检索到的具体内容未包含委托授权有效期，且委托事务未具有法定有效期，则确定委托事务的委托授权有效期为永久有效期。

[0046] 通过上述步骤S31-S33，对从区块链中检索到的委托事务的具体内容的委托授权有效期进行验证，以确保委托方真的委托受托方办理具体业务，且该委托授权在对应的授权有消息内。

[0047] 根据本申请实施例的委托授权验证方法，在执行方节点设备可以准确核实受托人的受托权限，确保受托方真正得到委托方的委托，从而保证确保委托人的利益免受不正当的损害。

[0048] 图2示出本申请另一实施例的委托授权验证方法的流程图。如图2所示，本申请实施例中的委托授权验证方法可以应用于委托方节点设备，并可以包括以下步骤。

[0049] S210，基于生成的委托事务的描述信息和委托事务的委托授权有效期，计算得到第一哈希值。

[0050] S220，为委托事务分配委托方索引号，对包含委托方索引号和第一哈希值的数据项进行委托方签名，并将委托方签名后的数据项发布到区块链中。

[0051] S230，根据委托方索引号、描述信息和委托授权有效期，得到委托事务的具体内容，对具体内容进行委托方签名，得到委托方签名后的具体内容。

[0052] S240,将委托方签名后的具体内容通过预定文件形式发送至受托方节点。

[0053] 其中,委托方签名后的具体内容,用于在受托方节点进行受托方签名后被发送至执行方节点,并且具体内容在执行方节点被用于与发布到区块链中的数据项进行哈希值的比对,以确定委托事务经过委托方的授权。

[0054] 通过上述步骤S210-S240,委托方节点设备可以将委托受托方办理业务的事项,进行签名后发布到区块链中,并将该委托受托方办理业务的事项,进行签名后直接发送给受托方,该委托方签名后的委托业务在受托方追加受托方签名后发送至执行方节点,从而在执行方节点执行委托事务之前,根据计算的从受托方收到的委托事项内容的哈希值,与从区块链上检索到的带有委托方签名的哈希值进行比较,根据比较结果确定受托方是否真正得到委托方的委托,确保委托人的利益免受不正当的损害。

[0055] 在一个实施例中,若委托事务的具体内容附带至少一个电子文件,则方法还包括步骤:S250,分别计算附带的每个电子文件的哈希值,得到第二哈希值,第二哈希值中包含每个电子文件的哈希值。

[0056] 步骤S220具体可以包括:S41,对包含委托方索引号、第一哈希值和第二哈希值的数据项进行委托方签名,经将委托方签名后的数据项发布到区块链中。

[0057] S230具体可以包括:S42,将委托方索引号、描述信息和委托授权有效期的委托事务的具体内容作为一个整体进行委托方签名,并对附带的每个电子文件进行委托方签名,得到委托方签名后的具体内容。

[0058] 在该实施例中,针对委托事务中附带的电子文件计算哈希值时,需要对每个电子文件单独计算其哈希值,相应地,对委托事务中附带的电子文件进行委托方签名时,需要对附带的每个电子文件依次进行委托方签名。

[0059] 在一个实施例中,若委托事务的具体内容附带至少一个电子文件,则委托方签名后的具体内容在受托方节点的签名包括如下签名项:在受托方节点为接收到的具体内容分配受托方申请编号后,并对申请编号进行的受托方签名;将具体内容中的委托方索引号、描述信息和委托授权有效期作为一个整体进行的受托方签名;以及,对附带的每个电子文件分别进行的受托方签名。

[0060] 根据本申请实施例的委托授权验证方法,委托方节点设备可以将委托受托方办理业务的事项,进行签名后发布到区块链中,并将该委托受托方办理业务的事项,进行签名后直接发送给受托方,该委托方签名后的委托业务在受托方追加受托方签名后发送至执行方节点,从而在执行方节点执行委托事务之前,根据计算的从受托方收到的委托事项内容的哈希值,与从区块链上检索到的带有委托方签名的哈希值进行比较,根据比较结果确定受托方是否真正得到委托方的委托,确保委托人的利益免受不正当的损害。

[0061] 为了更好的理解本申请,下面结合图3-图5,描述本申请示例性示例的委托授权验证方法。图3示出本申请示例性实施例中应用于委托方节点的委托授权验证的相关处理流程示意图;图4示出本申请示例性实施例中应用于受托方节点的委托授权验证的相关处理流程示意图;图5示出本申请示例性实施例中执行方节点的处理流程示意图。

[0062] 如图3所示,本申请示例性实施例中应用于委托方节点的委托授权验证的相关处理流程包括如下步骤。

[0063] S301,生成委托事务的具体内容,其中,该具体内容具体可以包括委托方身份说

明、受托方身份说明和委托事项的具体描述。

[0064] 在一些实施例中，若委托事务需要使用电子文件，则委托事务的具体内容还可以附带电子文档、图片、视频等电子形式的文件。

[0065] S302，将委托方身份说明、受托方身份说明、委托事项的具体描述和委托授权的有效期作为一个整体，计算哈希值，作为第一哈希值。

[0066] S303，若委托事务的具体内容附带电子文件，对每个电子文件单独计算哈希值，作为第二哈希值。

[0067] S304，为本次委托事务分配一个委托方索引号，以用于后续从区块链中根据该委托方索引号进行检索。

[0068] S305，将委托方索引号和第一哈希值和该第二哈希值作为一个整体，进行委托方签名后，发布到区块链上。

[0069] S306，委托方将委托方索引号、委托方身份说明、受托方身份说明、委托事项的具体描述、委托授权的有效期、附带的电子文件签名后，以电子形式直接发送给受托方节点。

[0070] 在一些实施例中，也可以以其他电子形式例如以加密电子邮件的形式将上述委托事务的具体内容发送给受托方，并且，可以将委托方索引号、委托方身份说明、受托方身份说明、委托事项的具体描述作为一个整体进行签名，附带的电子文件逐个单独进行委托方签名。

[0071] 通过上述步骤S305-S306，委托方节点设备将委托受托方办理业务的事项，进行签名后发布到区块链中，并将该委托受托方办理业务的事项，进行签名后直接发送给受托方，以进行后续受托方节点和执行方节点的相应处理，确保委托人的利益免受不正当的损害。

[0072] 如图4所示，本申请示例性实施例中应用于受托方节点的委托授权验证的相关处理流程包括如下步骤。

[0073] S401，在实际执行委托方所委托的事务之前，为委托方所委托的事务创建一个受托方申请编号。

[0074] S402，将受托方申请编号、从委托方接收到的委托事务的委托方索引编号、具体内容，进行受托方签名，并将追加受托方签名的委托事务的具体内容，以电子形式直接发给执行方节点。

[0075] 在步骤S402，对于追加受托方签名的委托事务的具体内容，也可以通过电子邮件的形式发给执行方节点设备。

[0076] 示例性地，将受托方节点设备为当前委托业务生成的申请编号，从委托方节点接收到的当前委托业务分配的索引号，以及从委托方节点接收到的当前委托业务的具体内容例如，以指定的电子形式发送至执行方节点设备。

[0077] 示例性地，当前委托业务的具体内容包括委托方身份说明、受托方身份说明、委托事项的具体描述和委托授权的有效期。在一个实施例中，根据实际应用场景中委托事项的具体需求，当前委托业务的具体内容还可以包括附带的电子文件。

[0078] S403，对委托方申请编号单独进行签名，并将委托方身份说明、受托方身份说明和委托事项的具体描述作为一个整体进行签名，以及对附带的电子文件逐个单独签名。

[0079] 通过上述步骤S401-S403，受托方将从委托方收到的内容追加自己的签名后发送给执行方。

[0080] 在本申请实施例的应用场景中，受托方可以持自身的身份证明文件例如身份证、护照、驾驶证等到执行方所在地，并向执行方出示身份证明文件和申请编号，以使执行方在实际执行委托事务之前，计算从受托方收到的内容的哈希值，并且此哈希值与从区块链上检索到的带有委托方签名的哈希值进行比较，根据比较结果确定是否可以在区块链上查找相同内容的记载，如果有，表示受托方确实是得到了委托方的委托，此时执行方即可执行受托方所请求的业务操作，确保委托人的利益免受不正当的损害。

[0081] 如图5所示，本申请示例性实施例中应用于执行方节点的委托授权验证的相关处理流程包括如下步骤。

[0082] S501，根据申请编号，在本地检索出受托方事前发送来的委托事务的具体内容，并分别验证其中的委托方签名和受托方签名。

[0083] S502，针对具体内容中的委托方身份说明、受托方身份说明、委托事项的具体描述、委托授权的有效期计算哈希值得到第一哈希值，若附带电子文件，则对每个附带电子文件单独计算其哈希值，得到第二哈希值。

[0084] S503，根据委托方索引号，在区块链账本上找到对应的数据项，验证所找到的数据项的签名的确为委托方的签名。

[0085] S504，对比区块链账本上找到的数据项与计算出的哈希值是否一一对应相同。

[0086] S505，确定当前日期是否在委托权限有效期内。

[0087] S506，若区块链账本上找到的数据项与计算出的哈希值一致，且当前日期在委托权限有效期内，确定委托事务经过委托方的授权。

[0088] 在一些实施例中，可以通过屏幕展示委托事务是否经过委托方的授权的验证结果，例如，若区块链账本上找到的数据项与计算出的哈希值一致，且当前日期在委托权限有效期内，则在屏幕上显示"验证通过"，证明受托方的确经过委托方的授权，否则，拒绝办理该委托事务，确保委托人的利益免受不正当的损害。

[0089] 在本申请实施例中，委托方、受托方、执行方均在区块链上完成了实名认证，本申请实施例对委托方、受托方、执行方在区块链上进行实名认证的具体过程不做具体限定。

[0090] 根据本申请实施例的委托授权验证方法，委托方将委托事务的描述信息和附加信息的哈希值签名并发布到区块链上，委托方将委托事务的描述信息和附加信息签名后直接发送给受托方，受托方将从委托方收到的内容追加自己的签名后发送给执行方，执行方在实际执行委托事务之前，计算从受托方收到的内容的哈希值，并且此哈希值与从区块链上检索到的带有委托方签名的哈希值进行比较，根据比较结果决定是否实际执行委托事务，从而确定委托事务在受托方在真正得到委托方的委托的情况下被执行，确保委托人的利益免受不正当的损害。

[0091] 下面结合附图，详细介绍根据本申请实施例的委托授权验证装置。图6示出根据本申请一实施例提供的委托授权验证装置的结构示意图。如图6所示，该委托授权验证装置包括如下模块。

[0092] 事务内容获取模块610，用于根据接收到的由受托方提供的申请编号，从预定数据库中检索由受托方预先发送到本节点设备的委托事务的具体内容，委托事务的具体内容至少包括受托方申请编号、委托方索引号和委托事务的描述信息；

[0093] 哈希值计算模块620，用于对具体内容携带的委托方签名和受托方签名进行验证

成功时，计算描述信息和获取的委托事务的委托授权有效期的哈希值；

[0094] 区块链查询模块630，用于从区块链中检索与委托方索引号对应的数据项，数据项是由委托方节点设备预先发布到区块链中的委托受托方办理的委托事务的数据项；

[0095] 比对验证模块640，用于对数据项携带的委托方签名进行验证成功时，若数据项所包含的哈希值与计算得到的哈希值相对应相同，则确定委托事务经过委托方的授权。

[0096] 根据本申请实施例的委托授权验证装置，执行方节点设备在实际执行委托事务之前，可以计算从受托方收到的内容的哈希值，并将此哈希值与从区块链上检索到的带有委托方签名的哈希值进行比较，根据比较结果确定受托方是否真正得到委托方的委托，确保委托人的利益免受不正当的损害。

[0097] 在一个实施例中，委托事务的具体内容携带的委托方签名和受托方签名包括第一签名、第二签名和第三签名；其中，第一签名是在委托方节点设备，将委托方索引号、描述信息和委托事务的委托授权有效期作为一个整体进行的签名；第二签名是在受托方节点设备，对受托方申请编号进行的签名，第三签名是在受托方节点设备，将委托方索引号、描述信息和委托授权有效期作为一个整体进行的签名。

[0098] 在该实施例中，哈希值计算模块620在用于对具体内容携带的委托方签名和受托方签名进行验证时，具体用于：根据受托方预先在区块链中完成的实名认证信息，验证第二签名和第三签名；根据委托方预先在区块链中完成的实名认证信息，验证第一签名。

[0099] 在一个实施例中，若委托事务的具体内容附带至少一个电子文件，则具体内容携带的委托方签名和受托方签名还包括第四签名和第五签名；其中，第四签名包括在委托方节点设备对附带的每个电子文件进行的签名，第五签名包括在受托方节点设备，对附带的每个电子文件进行的签名。

[0100] 在该实施例中，哈希值计算模块620在用于对具体内容携带的委托方签名和受托方签名进行验证时，具体用于：根据受托方预先在区块链中完成的实名认证信息，验证第五签名；根据委托方预先在区块链中完成的实名认证信息，验证第四签名。

[0101] 在一个实施例中，若委托事务的具体内容未附带电子文件，则数据项携带的委托方签名为第六签名，第六签名是在委托方节点设备，将委托方索引号和第一哈希值作为一个整体进行的签名；其中，第一哈希值是在委托方节点设备，将委托授权有效期和描述信息作为一个整体计算得到的哈希值；对数据项携带的委托方签名进行验证成功时，若数据项所包含的哈希值与计算得到的哈希值相对应相同。

[0102] 在该实施例中，比对验证模块640在确定委托事务经过委托方的授权时，具体用于：若验证第六签名成功，对委托授权有效期和描述信息进行哈希计算得到的哈希值与第一哈希值相同，且当前日期在委托授权有效期内，则确定委托事务经过委托方的授权。

[0103] 在一个实施例中，若委托事务的具体内容附带至少一个电子文件，则数据项携带的委托方签名为第七签名，第七签名是在委托方节点设备，将委托方索引号、第一哈希值和计算得到的第二哈希值作为一个整体进行的签名；其中，第二哈希值是分别对附带的每个电子文件进行计算得到的每个电子文件的哈希值。

[0104] 在一个实施例中，比对验证模块640，具体还用于：若验证第七签名成功，对委托授权有效期和描述信息进行哈希计算得到的哈希值与第一哈希值相同，对附带的每个电子文件计算的哈希值与第二哈希值对应相同，且当前日期在委托授权有效期内，则确定委托事

务经过委托方的授权。

[0105] 在一个实施例中，委托授权验证装置还包括委托授权有效期验证模块，用于在对具体内容携带的委托方签名和受托方签名进行验证之前，若检索到的具体内容包含委托授权有效期，则确定委托事务的委托授权有效期为检索到委托授权有效期；若检索到的具体内容未包含委托授权有效期，且委托事务具有法定有效期，则确定委托事务的委托授权有效期为法定有效期；若检索到的具体内容未包含委托授权有效期，且委托事务未具有法定有效期，则确定委托事务的委托授权有效期为永久有效期。

[0106] 根据本申请实施例的委托授权验证装置，在执行方节点设备可以准确核实受托人的受托权限，确保受托方真正得到委托方的委托，从而保证确保委托人的利益免受不正当的损害。

[0107] 图7示出了根据本申请另一实施例提供的委托授权验证装置的结构示意图。如图7所示，该委托授权验证装置包括如下模块。

[0108] 哈希值获取模块710，用于基于生成的委托事务的描述信息和委托事务的委托授权有效期，计算得到第一哈希值。

[0109] 数据项发布模块720，用于为委托事务分配委托方索引号，对包含委托方索引号和第一哈希值的数据项进行委托方签名，并将委托方签名后的数据项发布到区块链中。

[0110] 委托方签名模块730，用于根据委托方索引号、描述信息和委托授权有效期，得到委托事务的具体内容，对具体内容进行委托方签名，得到委托方签名后的具体内容。

[0111] 签名文件发送模块740，用于将委托方签名后的具体内容通过预定文件形式发送至受托方节点。

[0112] 在本申请实施例中，委托方签名后的具体内容，用于在受托方节点进行受托方签名后被发送至执行方节点，并且具体内容在执行方节点被用于与发布到区块链中的数据项进行哈希值的比对，以确定委托事务经过委托方的授权。

[0113] 在一个实施例中，若委托事务的具体内容附带至少一个电子文件，则哈希值计算模块710，还用于：分别计算附带的每个电子文件的哈希值，得到第二哈希值，第二哈希值中包含每个电子文件的哈希值；数据项发布模块720，还用于对包含委托方索引号、第一哈希值和第二哈希值的数据项进行委托方签名，经将委托方签名后的数据项发布到区块链中；委托方签名模块730，还用于将委托方索引号、描述信息和委托授权有效期的委托事务的具体内容作为一个整体进行委托方签名，并对附带的每个电子文件进行委托方签名，得到委托方签名后的具体内容。

[0114] 在一个实施例中，若委托事务的具体内容附带至少一个电子文件，则委托方签名后的具体内容在受托方节点的签名包括如下签名项：在受托方节点为接收到的具体内容分配受托方申请编号后，并对申请编号进行的受托方签名；将具体内容中的委托方索引号、描述信息和委托授权有效期作为一个整体进行的受托方签名；以及，对附带的每个电子文件分别进行的受托方签名。

[0115] 根据本申请实施例的委托授权验证装置，委托方节点设备可以将委托受托方办理业务的事项，进行签名后发布到区块链中，并将该委托受托方办理业务的事项，进行签名后直接发送给受托方，该委托方签名后的委托业务在受托方追加受托方签名后发送至执行方节点，从而在执行方节点执行委托事务之前，根据计算的从受托方收到的委托事项内容的

哈希值，与从区块链上检索到的带有委托方签名的哈希值，验证受托方是否真正得到委托方的委托，确保委托人的利益免受不正当的损害。

[0116] 需要明确的是，本申请并不局限于上文实施例中所描述并在图中示出的特定配置和处理。为了描述的方便和简洁，这里省略了对已知方法的详细描述，并且上述描述的系统、模块和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

[0117] 图8是示出能够实现根据本申请实施例的委托授权验证方法和装置的计算设备的示例性硬件架构的结构图。

[0118] 如图8所示，计算设备800包括输入设备801、输入接口802、中央处理器803、存储器804、输出接口805、以及输出设备806。其中，输入接口802、中央处理器803、存储器804、以及输出接口805通过总线810相互连接，输入设备801和输出设备806分别通过输入接口802和输出接口805与总线810连接，进而与计算设备800的其他组件连接。

[0119] 具体地，输入设备801接收来自外部的输入信息，并通过输入接口802将输入信息传送到中央处理器803；中央处理器803基于存储器804中存储的计算机可执行指令对输入信息进行处理以生成输出信息，将输出信息临时或者永久地存储在存储器804中，然后通过输出接口805将输出信息传送到输出设备806；输出设备806将输出信息输出到计算设备800的外部供用户使用。

[0120] 在一个实施例中，图8所示的计算设备800可以被实现为一种执行方节点设备，该委托方节点设备可以包括：存储器，被配置为存储程序；处理器，被配置为运行存储器中存储的程序，以执行上述实施例描述的应用于委托方节点设备的委托授权验证方法。

[0121] 在一个实施例中，图8所示的计算设备800可以被实现为一种受托方节点设备，该受托方节点设备可以包括：存储器，被配置为存储程序；处理器，被配置为运行存储器中存储的程序，以执行上述实施例描述的应用于受托方节点设备的委托授权验证方法。

[0122] 在一个实施例中，图8所示的计算设备800可以被实现为一种执行方节点设备，该执行方节点设备可以包括：存储器，被配置为存储程序；处理器，被配置为运行存储器中存储的程序，以执行上述实施例描述的应用于执行方节点设备的委托授权验证方法。

[0123] 根据本申请的实施例，上文参考流程图描述的过程可以被实现为计算机软件程序。例如，本申请的实施例包括一种计算机程序产品，其包括有形地包含在机器可读介质上的计算机程序，计算机程序包含用于执行流程图所示的方法的程序代码。在这样的实施例中，该计算机程序可以从网络上被下载和安装，和/或从可拆卸存储介质被安装。

[0124] 在上述实施例中，可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。当使用软件实现时，可以全部或部分地以计算机程序产品的形式实现。计算机程序产品包括一个或多个计算机指令，当其在计算机上运行时，使得计算机执行上述各个实施例中描述的方法。在计算机上加载和执行计算机程序指令时，全部或部分地产生按照本申请实施例的流程或功能。计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。计算机指令可以存储在计算机可读存储介质中，或者从一个计算机可读存储介质向另一个计算机可读存储介质传输，例如，计算机指令可以从一个网站站点、计算机、服务器或数据中心通过有线(例如同轴电缆、光纤、数字用户线(DSL))或无线(例如红外、无线、微波等)方式向另一个网站站点、计算机、服务器或数据中心进行传输。计算机可读存储介质可以是计算机能够存取的任何可用介质或者是包含一个或多个可用介质集成的服务器、数

据中心等数据存储设备。可用介质可以是磁性介质，(例如，软盘、硬盘、磁带)、光介质(例如，DVD)、或者半导体介质(例如固态硬盘)等。

[0125] 以上所描述的装置实施例仅仅是示意性的，其中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网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本实施例方案的目的。本领域普通技术人员在不付出创造性的劳动的情况下，即可以理解并实施。

[0126] 可以理解的是，以上实施方式仅仅是为了说明本申请的原理而采用的示例性实施方式，然而本申请并不局限于此。对于本领域内的普通技术人员而言，在不脱离本申请的精神和实质的情况下，可以做出各种变型和改进，这些变型和改进也视为本申请的保护范围。

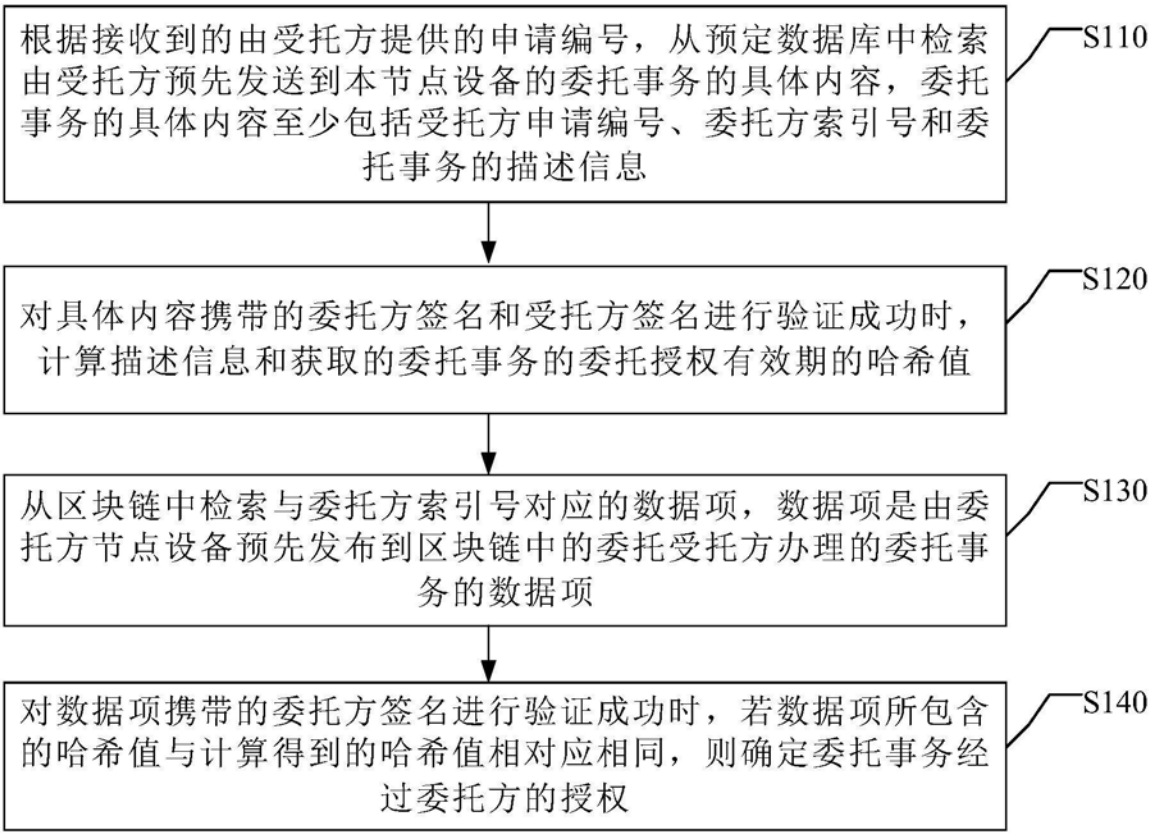

根据接收到的由受托方提供的申请编号，从预定数据库中检索由受托方预先发送到本节点设备的委托事务的具体内容，委托事务的具体内容至少包括受托方申请编号、委托方索引号和委托事务的描述信息
S110
对具体内容携带的委托方签名和受托方签名进行验证成功时，计算描述信息和获取的委托事务的委托授权有效期的哈希值
S120
从区块链中检索与委托方索引号对应的数据项，数据项是由委托方节点设备预先发布到区块链中的委托受托方办理的委托事务的数据项
S130
对数据项携带的委托方签名进行验证成功时，若数据项所包含的哈希值与计算得到的哈希值相对应相同，则确定委托事务经过委托方的授权
S140

图1

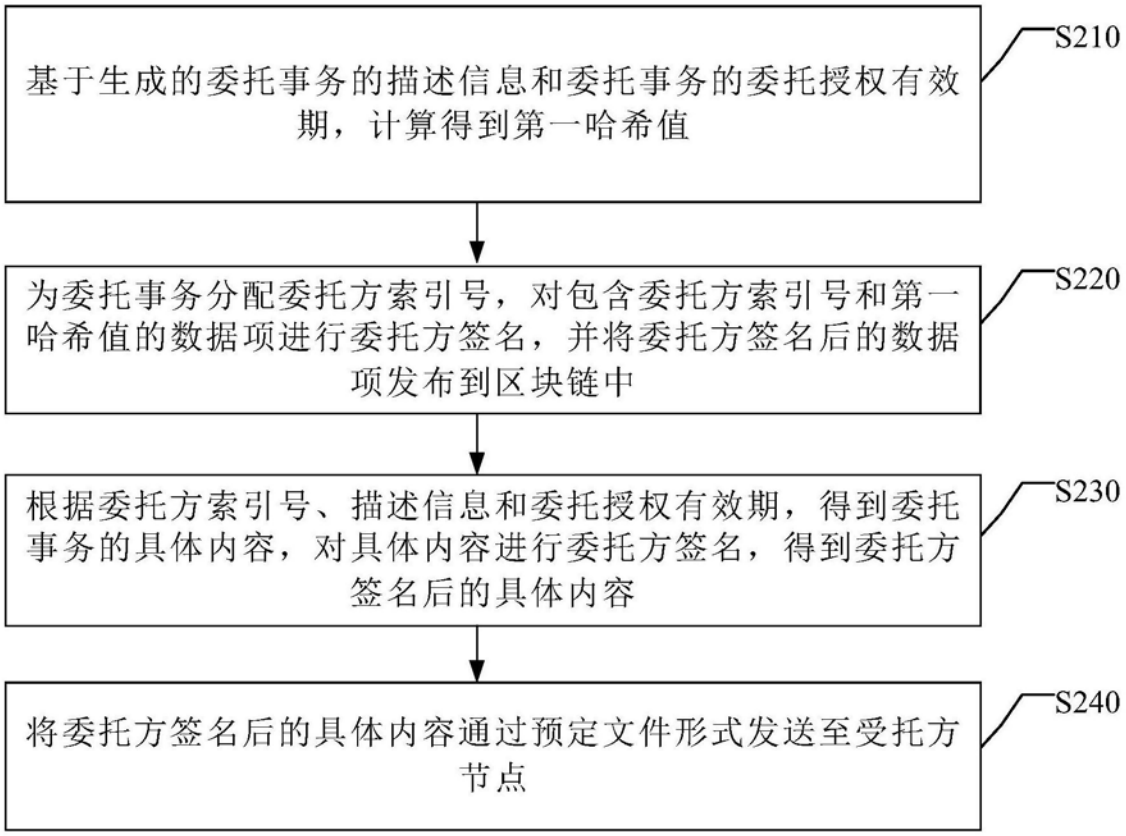

基于生成的委托事务的描述信息和委托事务的委托授权有效期，计算得到第一哈希值
S210
为委托事务分配委托方索引号，对包含委托方索引号和第一哈希值的数据项进行委托方签名，并将委托方签名后的数据项发布到区块链中
S220
根据委托方索引号、描述信息和委托授权有效期，得到委托事务的具体内容，对具体内容进行委托方签名，得到委托方签名后的具体内容
S230
将委托方签名后的具体内容通过预定文件形式发送至受托方节点
S240

图2

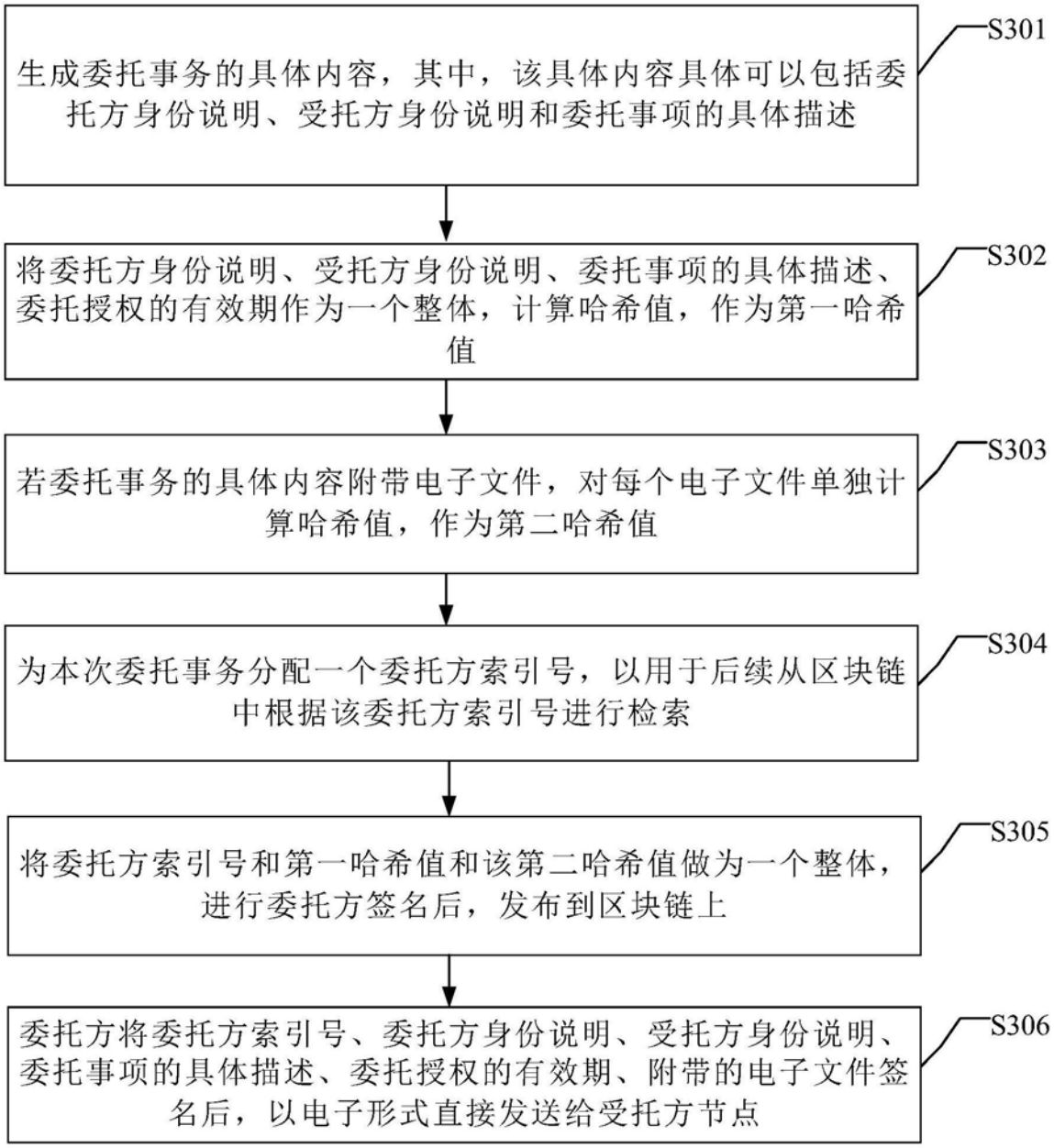

生成委托事务的具体内容，其中，该具体内容具体可以包括委托方身份说明、受托方身份说明和委托事项的具体描述
S301
将委托方身份说明、受托方身份说明、委托事项的具体描述、委托授权的有效期作为一个整体，计算哈希值，作为第一哈希值
S302
若委托事务的具体内容附带电子文件，对每个电子文件单独计算哈希值，作为第二哈希值
S303
为本次委托事务分配一个委托方索引号，以用于后续从区块链中根据该委托方索引号进行检索
S304
将委托方索引号和第一哈希值和该第二哈希值做为一个整体，进行委托方签名后，发布到区块链上
S305
委托方将委托方索引号、委托方身份说明、受托方身份说明、委托事项的具体描述、委托授权的有效期、附带的电子文件签名后，以电子形式直接发送给受托方节点
S306

图3

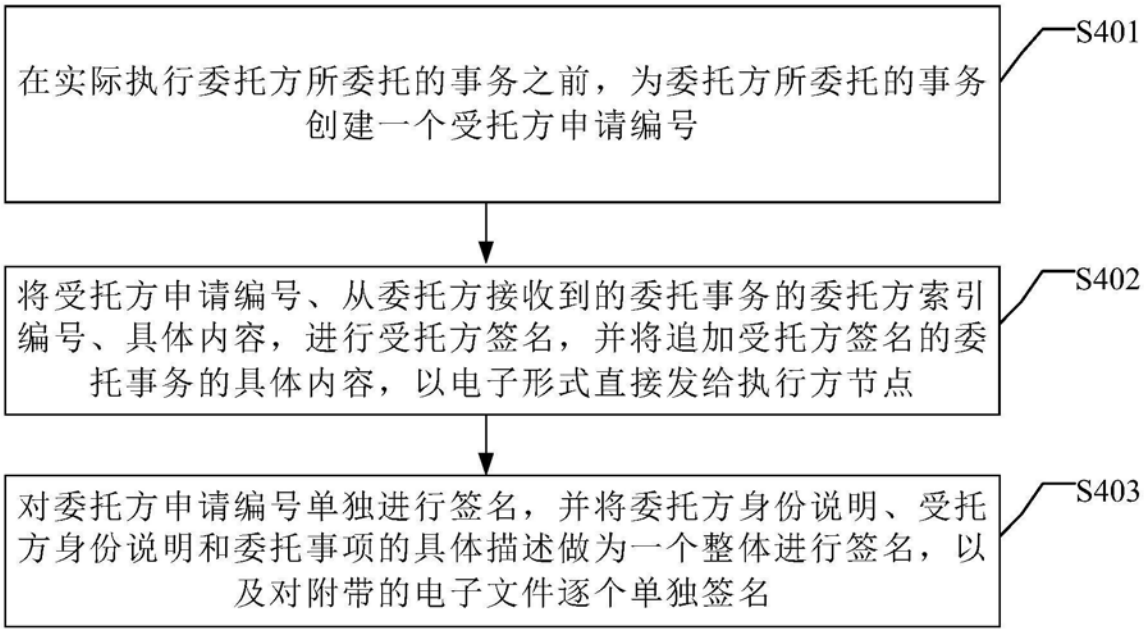

在实际执行委托方所委托的事务之前，为委托方所委托的事务创建一个受托方申请编号
S401
将受托方申请编号、从委托方接收到的委托事务的委托方索引编号、具体内容，进行受托方签名，并将追加受托方签名的委托事务的具体内容，以电子形式直接发给执行方节点
S402
对委托方申请编号单独进行签名，并将委托方身份说明、受托方身份说明和委托事项的具体描述做为一个整体进行签名，以及对附带的电子文件逐个单独签名
S403

图4

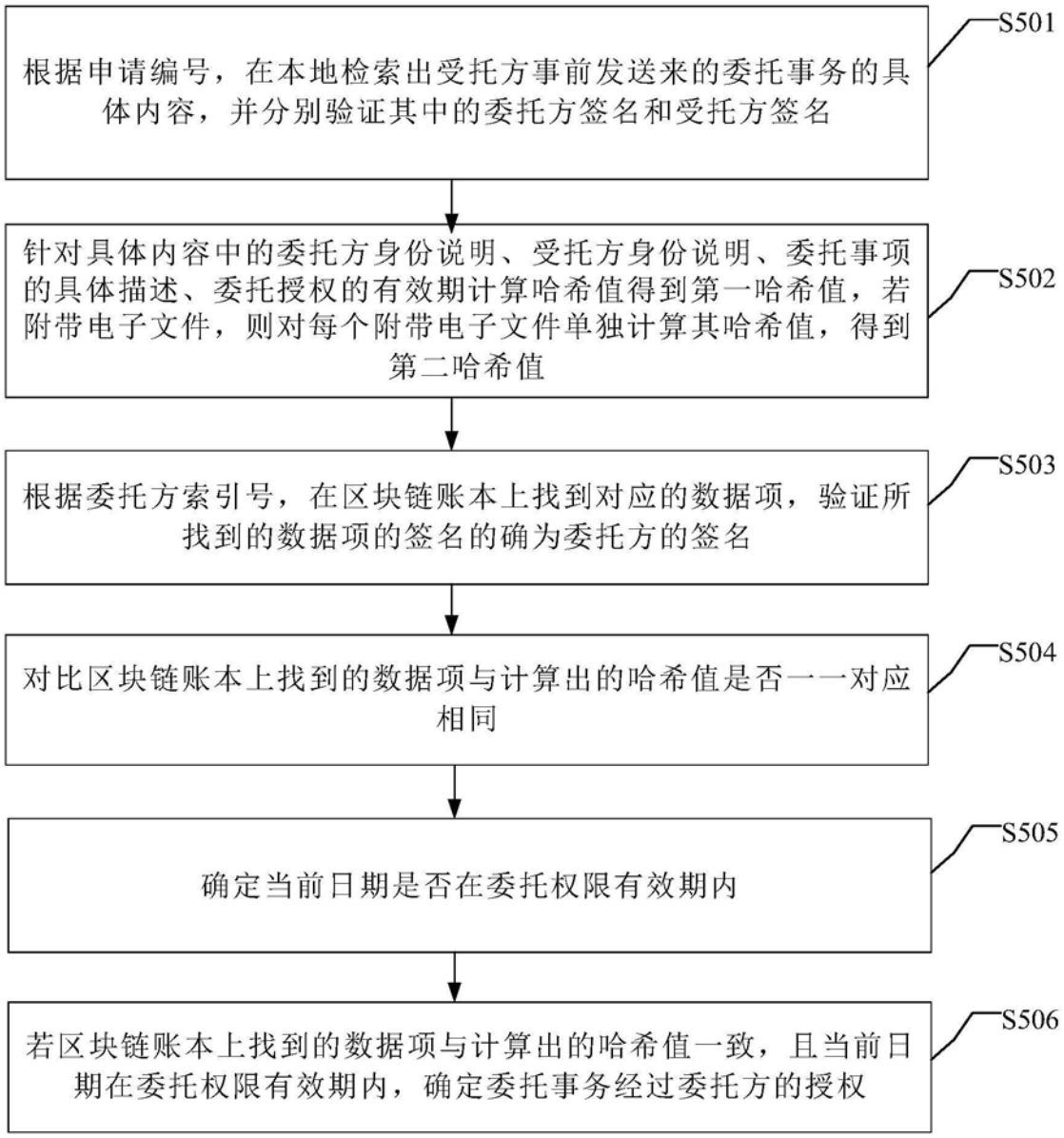

根据申请编号，在本地检索出受托方事前发送来的委托事务的具体内容，并分别验证其中的委托方签名和受托方签名
S501
针对具体内容中的委托方身份说明、受托方身份说明、委托事项的具体描述、委托授权的有效期计算哈希值得到第一哈希值，若附带电子文件，则对每个附带电子文件单独计算其哈希值，得到第二哈希值
S502
根据委托方索引号，在区块链账本上找到对应的数据项，验证所找到的数据项的签名的确为委托方的签名
S503
对比区块链账本上找到的数据项与计算出的哈希值是否一一对应相同
S504
确定当前日期是否在委托权限有效期内
S505
若区块链账本上找到的数据项与计算出的哈希值一致，且当前日期在委托权限有效期内，确定委托事务经过委托方的授权
S506

图5

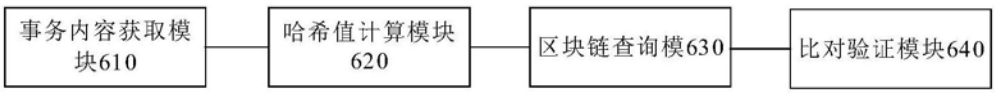

事务内容获取模块610
哈希值计算模块620
区块链查询模630
比对验证模块640

图6

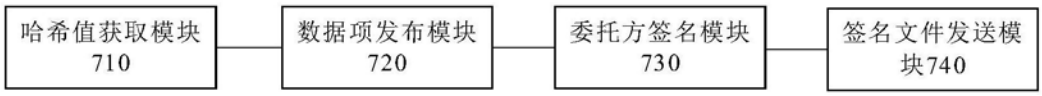

哈希值获取模块710
数据项发布模块720
委托方签名模块730
签名文件发送模块740

图7

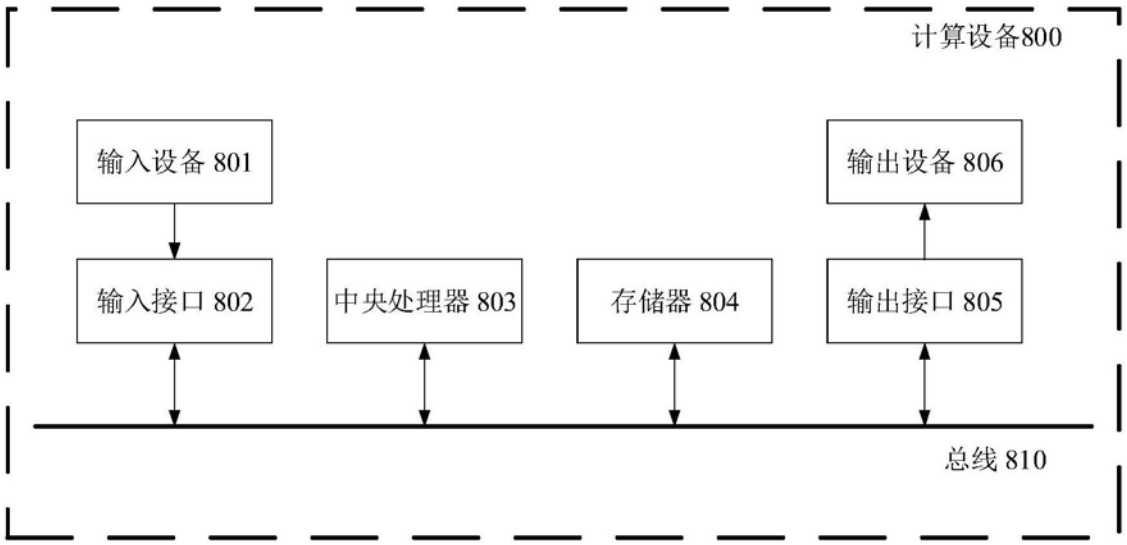

计算设备800
输入设备 801
输出设备 806
输入接口 802
中央处理器 803
存储器 804
输出接口 805
总线 810

图8