(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 110060111 A
(43)申请公布日 2019.07.26

(21)申请号 201811519422.4

(22)申请日 2018.12.12

(71)申请人 阿里巴巴集团控股有限公司
地址 英属开曼群岛大开曼资本大厦一座四层847号邮箱

(72)发明人 肖汉松 张萍 阚文虎 刘勤 林亮荣 邓福喜 张翼翔 陈锐 段金明

(74)专利代理机构 北京博思佳知识产权代理有限公司 11415
代理人 林祥

(51)Int.Cl.
G06Q 30/04(2012.01)
H04L 29/06(2006.01)

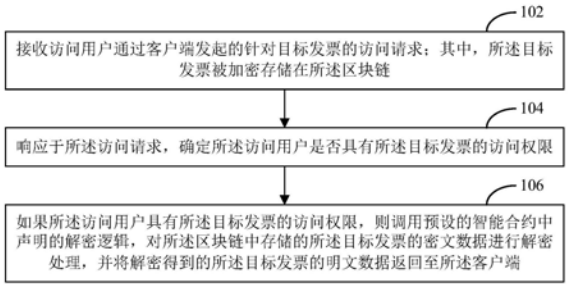
权利要求书3页 说明书13页 附图2页

(54)发明名称

基于区块链的发票访问方法和装置、电子设备

(57)摘要

本说明书一个或多个实施例提供一种基于区块链的发票访问方法和装置、电子设备，所述方法包括：接收访问用户通过客户端发起的针对目标发票的访问请求；其中，所述目标发票被加密存储在所述区块链中；响应于所述访问请求，确定所述访问用户是否具有所述目标发票的访问权限；如果所述访问用户具有所述目标发票的访问权限，则调用预设的智能合约中声明的解密逻辑，对所述区块链中存储的所述目标发票的密文数据进行解密处理，并将解密得到的所述目标发票的明文数据返回至所述客户端。



CN 110060111 A

1.一种基于区块链的发票访问方法,所述方法包括:

接收访问用户通过客户端发起的针对目标发票的访问请求;其中,所述目标发票被加密存储在所述区块链中;

响应于所述访问请求,确定所述访问用户是否具有所述目标发票的访问权限;

如果所述访问用户具有所述目标发票的访问权限,则调用预设的智能合约中声明的解密逻辑,对所述区块链中存储的所述目标发票的密文数据进行解密处理,并将解密得到的所述目标发票的明文数据返回至所述客户端。

2.根据权利要求1所述的方法,所述智能合约中还声明了针对所述访问用户的访问权限验证逻辑;

所述确定所述访问用户是否具有所述目标发票的访问权限,包括:

调用所述智能合约中声明的所述访问权限验证逻辑,确定所述访问用户是否具有所述目标发票的访问权限。

3.根据权利要求1或2所述的方法,所述方法还包括:

接收创建用户通过客户端发起的针对所述目标发票的创建请求;

响应于所述创建请求,确定所述目标发票的开票方和受票方;

调用所述智能合约中声明的加密逻辑,基于所述开票方和受票方对应的密钥,分别对所述目标发票的明文数据进行加密处理,并将加密得到的所述目标发票的密文数据,以及所述目标发票的开票方和受票方的用户标识发布至所述区块链中进行存储。

4.根据权利要求3所述的方法,所述基于所述开票方和受票方对应的密钥,分别对所述目标发票的明文数据进行加密处理,包括:

基于所述开票方对应的密钥,对所述目标发票的明文数据进行加密处理,得到第一密文数据;

基于所述受票方对应的密钥,对所述目标发票的明文数据进行加密处理,得到第二密文数据;

将加密得到的所述目标发票的密文数据,以及所述目标发票的开票方和受票方的用户标识发布至所述区块链中进行存储,包括:

将所述第一密文数据与所述开票方的用户标识的对应关系发布至所述区块链中进行存储;

将所述第二密文数据与所述受票方的用户标识的对应关系发布至所述区块链中进行存储。

5.根据权利要求3所述的方法,所述访问请求中包括所述访问用户的用户标识;

所述确定所述访问用户是否具有所述目标发票的访问权限,包括:

获取所述目标发票的开票方和受票方的用户标识;

判断所述访问用户的用户标识与所述开票方和受票方的用户标识是否匹配;

如果所述访问用户的用户标识与所述开票方和受票方的用户标识匹配,则确定所述访问用户具有所述目标发票的访问权限。

6.根据权利要求3所述的方法,所述对所述区块链中存储的所述目标发票的密文数据进行解密处理,包括:

基于所述访问用户对应的密钥,对所述区块链中存储的所述目标发票的密文数据进行

解密处理。

7.根据权利要求3所述的方法,所述智能合约中还声明了密钥分配逻辑;

所述方法还包括:

接收用户通过客户端发起的注册请求;

响应于所述注册请求,调用所述智能合约中的所述密钥分配逻辑,将所述用户的用户标识和为所述用户分配的密钥的对应关系写入所述智能合约。

8.根据权利要求3所述的方法,所述用户标识为纳税人识别号。

9.一种基于区块链的发票访问装置,所述装置包括:

第一接收模块,用于接收访问用户通过客户端发起的针对目标发票的访问请求;其中,所述目标发票被加密存储在所述区块链中;

第一确定模块,用于响应于所述访问请求,确定所述访问用户是否具有所述目标发票的访问权限;

解密模块,用于在所述访问用户具有所述目标发票的访问权限时,调用预设的智能合约中声明的解密逻辑,对所述区块链中存储的所述目标发票的密文数据进行解密处理,并将解密得到的所述目标发票的明文数据返回至所述客户端。

10.根据权利要求9所述的装置,所述智能合约中还声明了针对所述访问用户的访问权限验证逻辑;

所述第一确定模块具体用于:

调用所述智能合约中声明的所述访问权限验证逻辑,确定所述访问用户是否具有所述目标发票的访问权限。

11.根据权利要求9或10所述的装置,所述装置还包括:

第二接收模块,用于接收创建用户通过客户端发起的针对所述目标发票的创建请求;

第二确定模块,用于响应于所述创建请求,确定所述目标发票的开票方和受票方;

加密模块,用于调用所述智能合约中声明的加密逻辑,基于所述开票方和受票方对应的密钥,分别对所述目标发票的明文数据进行加密处理,并将加密得到的所述目标发票的密文数据,以及所述目标发票的开票方和受票方的用户标识发布至所述区块链中进行存储。

12.根据权利要求11所述的装置,所述加密模块具体用于:

基于所述开票方对应的密钥,对所述目标发票的明文数据进行加密处理,得到第一密文数据;

基于所述受票方对应的密钥,对所述目标发票的明文数据进行加密处理,得到第二密文数据;

将加密得到的所述目标发票的密文数据,以及所述目标发票的开票方和受票方的用户标识发布至所述区块链中进行存储,包括:

将所述第一密文数据与所述开票方的用户标识的对应关系发布至所述区块链中进行存储;

将所述第二密文数据与所述受票方的用户标识的对应关系发布至所述区块链中进行存储。

13.根据权利要求11所述的装置,所述访问请求中包括所述访问用户的用户标识;

所述第一确定模块具体用于：

获取所述目标发票的开票方和受票方的用户标识；

判断所述访问用户的用户标识与所述开票方和受票方的用户标识是否匹配；

如果所述访问用户的用户标识与所述开票方和受票方的用户标识匹配，则确定所述访问用户具有所述目标发票的访问权限。

14.根据权利要求11所述的装置，所述解密模块具体用于：

基于所述访问用户对应的密钥，对所述区块链中存储的所述目标发票的密文数据进行解密处理。

15.根据权利要求11所述的装置，所述智能合约中还声明了密钥分配逻辑；

所述装置还包括：

第三接收模块，用于接收用户通过客户端发起的注册请求；

注册模块，用于响应于所述注册请求，调用所述智能合约中的所述密钥分配逻辑，将所述用户的用户标识和为所述用户分配的密钥的对应关系写入所述智能合约。

16.根据权利要求11所述的装置，所述用户标识为纳税人识别号。

17.一种电子设备，所述电子设备包括：

处理器；

用于存储机器可执行指令的存储器；

其中，通过读取并执行所述存储器存储的与基于区块链的发票访问的控制逻辑对应的机器可执行指令，所述处理器被促使：

接收访问用户通过客户端发起的针对目标发票的访问请求；其中，所述目标发票被加密存储在所述区块链中；

响应于所述访问请求，确定所述访问用户是否具有所述目标发票的访问权限；

如果所述访问用户具有所述目标发票的访问权限，则调用预设的智能合约中声明的解密逻辑，对所述区块链中存储的所述目标发票的密文数据进行解密处理，并将解密得到的所述目标发票的明文数据返回至所述客户端。

基于区块链的发票访问方法和装置、电子设备

技术领域

[0001] 本说明书一个或多个实施例涉及区块链技术领域，尤其涉及一种基于区块链的发票访问方法和装置、电子设备。

背景技术

[0002] 区块链技术，也被称之为分布式账本技术，是一种由若干台计算设备共同参与“记账”，共同维护一份完整的分布式数据库的新兴技术。由于区块链技术具有去中心化、公开透明、每台计算设备可以参与数据库记录、并且各计算设备之间可以快速的进行数据同步的特性，利用区块链技术来搭建去中心化系统，并在区块链的分布式数据库中收录各种执行程序进行自动执行，已在众多的领域中广泛的进行应用。

发明内容

[0003] 本说明书提出一种基于区块链的发票访问方法，所述方法包括：

[0004] 接收访问用户通过客户端发起的针对目标发票的访问请求；其中，所述目标发票被加密存储在所述区块链中；

[0005] 响应于所述访问请求，确定所述访问用户是否具有所述目标发票的访问权限；

[0006] 如果所述访问用户具有所述目标发票的访问权限，则调用预设的智能合约中声明的解密逻辑，对所述区块链中存储的所述目标发票的密文数据进行解密处理，并将解密得到的所述目标发票的明文数据返回至所述客户端。

[0007] 可选地，所述智能合约中还声明了针对所述访问用户的访问权限验证逻辑；

[0008] 所述确定所述访问用户是否具有所述目标发票的访问权限，包括：

[0009] 调用所述智能合约中声明的所述访问权限验证逻辑，确定所述访问用户是否具有所述目标发票的访问权限。

[0010] 可选地，所述方法还包括：

[0011] 接收创建用户通过客户端发起的针对所述目标发票的创建请求；

[0012] 响应于所述创建请求，确定所述目标发票的开票方和受票方；

[0013] 调用所述智能合约中声明的加密逻辑，基于所述开票方和受票方对应的密钥，分别对所述目标发票的明文数据进行加密处理，并将加密得到的所述目标发票的密文数据，以及所述目标发票的开票方和受票方的用户标识发布至所述区块链中进行存储。

[0014] 可选地，所述基于所述开票方和受票方对应的密钥，分别对所述目标发票的明文数据进行加密处理，包括：

[0015] 基于所述开票方对应的密钥，对所述目标发票的明文数据进行加密处理，得到第一密文数据；

[0016] 基于所述受票方对应的密钥，对所述目标发票的明文数据进行加密处理，得到第二密文数据；

[0017] 将加密得到的所述目标发票的密文数据，以及所述目标发票的开票方和受票方的

用户标识发布至所述区块链中进行存储，包括：

[0018] 将所述第一密文数据与所述开票方的用户标识的对应关系发布至所述区块链中进行存储；

[0019] 将所述第二密文数据与所述受票方的用户标识的对应关系发布至所述区块链中进行存储。

[0020] 可选地，所述访问请求中包括所述访问用户的用户标识；

[0021] 所述确定所述访问用户是否具有所述目标发票的访问权限，包括：

[0022] 获取所述目标发票的开票方和受票方的用户标识；

[0023] 判断所述访问用户的用户标识与所述开票方和受票方的用户标识是否匹配；

[0024] 如果所述访问用户的用户标识与所述开票方和受票方的用户标识匹配，则确定所述访问用户具有所述目标发票的访问权限。

[0025] 可选地，所述对所述区块链中存储的所述目标发票的密文数据进行解密处理，包括：

[0026] 基于所述访问用户对应的密钥，对所述区块链中存储的所述目标发票的密文数据进行解密处理。

[0027] 可选地，所述智能合约中还声明了密钥分配逻辑；

[0028] 所述方法还包括：

[0029] 接收用户通过客户端发起的注册请求；

[0030] 响应于所述注册请求，调用所述智能合约中的所述密钥分配逻辑，将所述用户的用户标识和为所述用户分配的密钥的对应关系写入所述智能合约。

[0031] 可选地，所述用户标识为纳税人识别号。

[0032] 本说明书还提出一种基于区块链的发票访问装置，所述装置包括：

[0033] 第一接收模块，用于接收访问用户通过客户端发起的针对目标发票的访问请求；其中，所述目标发票被加密存储在所述区块链中；

[0034] 第一确定模块，用于响应于所述访问请求，确定所述访问用户是否具有所述目标发票的访问权限；

[0035] 解密模块，用于在所述访问用户具有所述目标发票的访问权限时，调用预设的智能合约中声明的解密逻辑，对所述区块链中存储的所述目标发票的密文数据进行解密处理，并将解密得到的所述目标发票的明文数据返回至所述客户端。

[0036] 可选地，所述智能合约中还声明了针对所述访问用户的访问权限验证逻辑；

[0037] 所述第一确定模块具体用于：

[0038] 调用所述智能合约中声明的所述访问权限验证逻辑，确定所述访问用户是否具有所述目标发票的访问权限。

[0039] 可选地，所述装置还包括：

[0040] 第二接收模块，用于接收创建用户通过客户端发起的针对所述目标发票的创建请求；

[0041] 第二确定模块，用于响应于所述创建请求，确定所述目标发票的开票方和受票方；

[0042] 加密模块，用于调用所述智能合约中声明的加密逻辑，基于所述开票方和受票方对应的密钥，分别对所述目标发票的明文数据进行加密处理，并将加密得到的所述目标发

票的密文数据，以及所述目标发票的开票方和受票方的用户标识发布至所述区块链中进行存储。

[0043] 可选地，所述加密模块具体用于：

[0044] 基于所述开票方对应的密钥，对所述目标发票的明文数据进行加密处理，得到第一密文数据；

[0045] 基于所述受票方对应的密钥，对所述目标发票的明文数据进行加密处理，得到第二密文数据；

[0046] 将加密得到的所述目标发票的密文数据，以及所述目标发票的开票方和受票方的用户标识发布至所述区块链中进行存储，包括：

[0047] 将所述第一密文数据与所述开票方的用户标识的对应关系发布至所述区块链中进行存储；

[0048] 将所述第二密文数据与所述受票方的用户标识的对应关系发布至所述区块链中进行存储。

[0049] 可选地，所述访问请求中包括所述访问用户的用户标识；

[0050] 所述第一确定模块具体用于：

[0051] 获取所述目标发票的开票方和受票方的用户标识；

[0052] 判断所述访问用户的用户标识与所述开票方和受票方的用户标识是否匹配；

[0053] 如果所述访问用户的用户标识与所述开票方和受票方的用户标识匹配，则确定所述访问用户具有所述目标发票的访问权限。

[0054] 可选地，所述解密模块具体用于：

[0055] 基于所述访问用户对应的密钥，对所述区块链中存储的所述目标发票的密文数据进行解密处理。

[0056] 可选地，所述智能合约中还声明了密钥分配逻辑；

[0057] 所述装置还包括：

[0058] 第三接收模块，用于接收用户通过客户端发起的注册请求；

[0059] 注册模块，用于响应于所述注册请求，调用所述智能合约中的所述密钥分配逻辑，将所述用户的用户标识和为所述用户分配的密钥的对应关系写入所述智能合约。

[0060] 可选地，所述用户标识为纳税人识别号。

[0061] 本说明书还提出一种电子设备，所述电子设备包括：

[0062] 处理器；

[0063] 用于存储机器可执行指令的存储器；

[0064] 其中，通过读取并执行所述存储器存储的与基于区块链的发票访问的控制逻辑对应的机器可执行指令，所述处理器被促使：

[0065] 接收访问用户通过客户端发起的针对目标发票的访问请求；其中，所述目标发票被加密存储在所述区块链中；

[0066] 响应于所述访问请求，确定所述访问用户是否具有所述目标发票的访问权限；

[0067] 如果所述访问用户具有所述目标发票的访问权限，则调用预设的智能合约中声明的解密逻辑，对所述区块链中存储的所述目标发票的密文数据进行解密处理，并将解密得到的所述目标发票的明文数据返回至所述客户端。

[0068] 在上述技术方案中，在用户需要访问被加密存储的区块链中的发票时，可以通过调用部署在该区块链上的智能合约中相应的逻辑，实现对该用户进行访问权限验证，并在确定该用户具有该发票的访问权限时，允许该用户访问该发票。采用这样的方式，可以保证在区块链上流转的发票的数据安全性，避免发票数据泄露而导致安全隐患。

附图说明

[0069] 图1是本说明书一示例性实施例示出的一种基于区块链的发票访问方法的流程图；

[0070] 图2是本说明书一示例性实施例示出的另一种基于区块链的发票访问方法的流程图；

[0071] 图3是本说明书一示例性实施例示出的一种基于区块链的发票访问装置所在电子设备的硬件结构图；

[0072] 图4是本说明书一示例性实施例示出的一种基于区块链的发票访问装置的框图。

具体实施方式

[0073] 这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本说明书一个或多个实施例相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本说明书一个或多个实施例的一些方面相一致的装置和方法的例子。

[0074] 在本说明书使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本说明书。在本说明书和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式，除非上下文清楚地表示其他含义。还应当理解，本文中使用的术语“和/或”是指并包含一个或多个相关联的列出项目的任何或所有可能组合。

[0075] 应当理解，尽管在本说明书可能采用术语第一、第二、第三等来描述各种信息，但这些信息不应限于这些术语。这些术语仅用来将同一类型的信息彼此区分开。例如，在不脱离本说明书范围的情况下，第一信息也可以被称为第二信息，类似地，第二信息也可以被称为第一信息。取决于语境，如在此所使用的词语“如果”可以被解释成为“在……时”或“当……时”或“响应于确定”。

[0076] 本说明书旨在提供一种在用户访问被加密存储在区块链中的发票时，通过调用部署在该区块链上的智能合约中相应的逻辑，以对该用户进行访问权限验证，并在确定该用户具有该发票的访问权限时，允许该用户访问该发票的技术方案。

[0077] 在具体实现时，发票通常会被加密存储在区块链中，即发票通常以密文的形式存储在该区块链中。用户在需要访问存储在区块链中的某张发票时，可以通过客户端发起针对该发票的访问请求。

[0078] 该区块链中的节点设备在接收到该访问请求后，可以对该访问请求进行响应。

[0079] 具体地，可以先确定该用户是否具有该发票的访问权限。对于某张发票来说，通常仅会允许该发票的开票方和受票方访问该发票，而不允许其他用户访问该发票，以保证发票的数据安全性，避免发票数据泄露。在这种情况下，可以先确定该用户是否为该发票的开

票方或受票方。如果该用户是该发票的开票方或受票方，则可以确定该用户具有该发票的访问权限。

[0080] 在确定了该用户具有该发票的访问权限后，该节点设备可以调用部署在该区块链上的智能合约中的解密逻辑，对该区块链中存储的该发票的密文数据进行解密处理，得到该发票的明文数据。

[0081] 在得到了该发票的明文数据后，该节点设备可以将该发票的明文数据返回至该客户端，从而使该客户端可以基于该发票的明文数据进行后续的业务处理；例如，该客户端可以将该发票的明文数据展示给该访问用户，以供该访问用户查看。

[0082] 在上述技术方案中，在用户需要访问被加密存储的区块链中的发票时，可以通过调用部署在该区块链上的智能合约中相应的逻辑，实现对该用户进行访问权限验证，并在确定该用户具有该发票的访问权限时，允许该用户访问该发票。采用这样的方式，可以保证在区块链上流转的发票的数据安全性，避免发票数据泄露而导致安全隐患。

[0083] 下面通过具体实施例对本说明书进行描述。

[0084] 请参考图1，图1是本说明书一示例性实施例示出的一种基于区块链的发票访问方法的流程图。该方法可以应用于区块链中的节点设备，包括如下步骤：

[0085] 步骤102，接收访问用户通过客户端发起的针对目标发票的访问请求；其中，所述目标发票被加密存储在所述区块链；

[0086] 步骤104，响应于所述访问请求，确定所述访问用户是否具有所述目标发票的访问权限；

[0087] 步骤106，如果所述访问用户具有所述目标发票的访问权限，则调用预设的智能合约中声明的解密逻辑，对所述区块链中存储的所述目标发票的密文数据进行解密处理，并将解密得到的所述目标发票的明文数据返回至所述客户端。

[0088] 在本说明书中描述的区块链，具体可以包括任意类型的区块链网络；例如，在实际应用中，可以采用共有链、私有链、或者联盟链中的任意一种。

[0089] 在本实施例中，发票通常可以被加密存储在区块链中，即发票通常以密文的形式存储在该区块链中。

[0090] 访问用户在需要访问存储在该区块链中的目标发票时，可以通过其所使用的客户端发起一笔用于访问该发票的交易，即通过客户端发起针对该发票的访问请求。

[0091] 其中，区块链中的交易，存在狭义的交易以及广义的交易之分。狭义的交易是指用户向区块链发布的一笔价值转移；例如，在传统的比特币区块链网络中，交易可以是用户在区块链中发起的一笔转账。而广义的交易是指用户向区块链发布的一笔具有业务意图的业务数据；例如，运营方可以基于实际的业务需求搭建一个联盟链，依托于联盟链部署一些与价值转移无关的其它类型的在线业务(比如，租房业务、车辆调度业务、保险理赔业务、信用服务、医疗服务等)，而在这类联盟链中，交易可以是用户在联盟链中发布的一笔具有业务意图的业务消息或者业务请求。

[0092] 需要说明的是，用户具体可以是个人，也可以是企业，本说明书对此不作限制。

[0093] 该区块链中的节点设备在接收到该访问请求后，可以对该访问请求进行响应。

[0094] 具体地，可以先确定该访问用户是否具有该目标发票的访问权限。

[0095] 如果确定该访问用户具有该目标发票的访问权限，则可以调用部署在该区块链上

的智能合约中声明的解密逻辑，对该区块链中的存储的该目标发票的密文数据进行解密处理，以得到该目标发票的明文数据。

[0096] 其中，解密逻辑具体可以是声明在该智能合约中的，与对发票的密文数据进行解密处理的执行逻辑相关的程序代码(例如：一些可供调用的程序方法或者函数)。

[0097] 在解密得到该目标发票的明文数据后，即可将该目标发票的明文数据返回至该客户端，从而使该客户端可以基于该目标发票的明文数据进行后续的业务处理；例如，该客户端可以对该目标发票的明文数据按照发票的标准格式进行整理，并将整理得到的该目标发票展示给该访问用户，以供该访问用户查看。

[0098] 在实际应用中，上述智能合约中还可以声明针对该访问用户的访问权限验证逻辑。在这种情况下，可以调用该智能合约中的访问权限验证逻辑，以确定所述访问用户是否具有所述目标发票的访问权限。

[0099] 其中，访问权限验证逻辑具体可以是声明在该智能合约中的，与对访问用户的访问权限进行验证的执行逻辑相关的程序代码。

[0100] 另一方面，请参考图2，可以采用如下步骤实现将上述目标发票加密后存储在上述区块链中：

[0101] 步骤202，接收创建用户通过客户端发起的针对所述目标发票的创建请求；

[0102] 步骤204，响应于所述创建请求，确定所述目标发票的开票方和受票方；

[0103] 步骤206，调用所述智能合约中声明的加密逻辑，基于所述开票方和受票方对应的密钥，分别对所述目标发票的明文数据进行加密处理，并将加密得到的所述目标发票的密文数据，以及所述目标发票的开票方和受票方的用户标识发布至所述区块链中进行存储。

[0104] 在本实施例中，创建用户可以通过其所使用的客户端发起针对上述目标发票的创建请求。

[0105] 该区块链中的节点设备在接收到该创建请求后，可以响应于该创建请求，先确定该目标发票的开票方和受票方。在实际应用中，该目标发票的开票方通常为该创建用户。

[0106] 在确定了该目标发票的开票方和受票方后，可以调用部署在该区块链上的智能合约中的加密逻辑，基于该开票方和该受票方对应的密钥，分别对该目标发票的明文数据进行加密处理，以得到该目标发票的密文数据。

[0107] 其中，加密逻辑具体可以是声明在该智能合约中的，与对发票的明文数据进行加密处理的执行逻辑相关的程序代码。

[0108] 在加密得到的该目标发票的密文数据后，可以将该目标发票的密文数据和该目标发票的开票方和受票方的用户标识发布至该区块链中进行存储。其中，用户标识通常可以是纳税人识别号。

[0109] 具体地，可以将该目标发票的密文数据和该目标发票的开票方和受票方的用户标识发送给该区块链中的节点设备，该区块链中的节点设备在接收到该密文数据和该用户标识后，可以发起对该密文数据和该用户标识的共识，并在共识通过后，存储该密文数据和该用户标识，从而实现将该密文数据和该用户标识发布至该区块链中进行存储。

[0110] 需要说明的是，以上描述的用于对区块链中存储的发票的密文数据进行解密处理的智能合约，和用于对发票的明文数据进行加密处理并发布至该区块链中进行存储的智能合约，可以整合为一个智能合约在上述区块链上进行部署，也可以作为两个不同的智能合

约在该区块链上进行部署，本说明书对此不作限定。

[0111] 在实际应用中，上述智能合约中还可以声明针对上述目标发票的用户身份确认逻辑。在这种情况下，可以调用该智能合约中的用户身份确认逻辑，以确定该目标发票的开票方和受票方。

[0112] 其中，用户身份确认逻辑具体可以是声明在该智能合约中的，与确定发票的开票方和受票方的执行逻辑相关的程序代码。

[0113] 举例来说，该创建请求中通常可以包括该创建用户在创建该目标发票时输入的开票方和受票方的用户标识，即可以将该创建用户输入的开票方的用户标识确定为该目标发票的开票方的用户标识，将该创建用户输入的受票方的用户标识确定为该目标发票的受票方的用户标识，从而实现确定该目标发票的开票方和受票方。

[0114] 在示出的一种实施方式中，为了实现对上述目标发票的明文数据进行加密处理，一方面，可以基于该开票方对应的密钥，对该目标发票的明文数据进行加密处理，得到该开票方对应的该目标发票的密文数据(称为第一密文数据)；另一方面，可以基于该受票方对应的密钥，对该目标发票的明文数据进行加密处理，得到该受票方对应的该目标发票的密文数据(称为第二密文数据)。

[0115] 后续，可以将该第一密文数据与该开票方的用户标识的对应关系发布至该区块链中进行存储，并将该第二密文数据与该受票方的用户标识的对应关系发布至该区块链中进行存储。

[0116] 具体地，该目标发票的密文数据的存储形式可以如下表1所示：

[0117]

密文数据1	用户标识1	密文数据2	用户标识2

[0118] 表1

[0119] 在上表1中，密文数据1为该开票方对应的该目标发票的密文数据，即为该第一密文数据，用户标识1为该开票方的用户标识；密文数据2为该受票方对应的该目标发票的密文数据，即为该第二密文数据，用户标识2为该受票方的用户标识。

[0120] 结合图2所示的实施例，继续参考图1，在示出的一种实施方式中，上述访问用户通过其所使用的客户端发起的针对上述目标发票的访问请求，其中可以包括该访问用户的用户标识。

[0121] 在这种情况下，为了确定该访问用户是否具有该目标发票的访问权限，可以先获取该目标发票的开票方和受票方的用户标识。

[0122] 在获取到该开票方和该受票方的用户标识后，一方面，可以将该访问用户的用户标识和该开票方的用户标识进行对比；另一方面，可以将该访问用户的用户标识和该受票方的用户标识进行对比，以判断该访问用户的用户标识与该开票方和该受票方的用户标识是否匹配。

[0123] 如果该访问用户的用户标识与该开票方和该受票方的用户标识匹配，则可以确定该访问用户具有该目标发票的访问权限。具体地，如果该访问用户的用户标识与该开票方的用户标识相同，则说明该访问用户是该目标发票的开票方，具有该目标发票的访问权限；如果该访问用户的用户标识与该受票方的用户标识相同，则说明该访问用户是该目标发票的受票方，也具有该目标发票的访问权限。

[0124] 在确定了该访问用户具有该目标发票的访问权限后，可以基于该访问用户对应的密钥，对上述区块链中的存储的该目标发票的密文数据进行解密处理，以得到该目标发票的明文数据。

[0125] 在实际应用中，上述智能合约中还可以声明针对用户的密钥分配逻辑。在这种情况下，对于任一用户而言，都可以通过客户端发起注册请求。

[0126] 其中，密钥分配逻辑具体可以是声明在该智能合约中的，与为用户分配密钥的执行逻辑相关的程序代码。

[0127] 上述区块链中的节点设备在接收到该注册请求后，可以响应于该注册请求，调用该智能合约中的密钥分配逻辑，以为该用户分配密钥，并将该用户的用户标识(通常可以包含在该注册请求中)和为该用户分配的密钥的对应关系写入该智能合约。

[0128] 即该智能合约中可以存储如下表2所示的对应关系：

[0129]

用户标识1	密钥1
用户标识2	密钥2
用户标识3	密钥3
……	……

[0130] 表2

[0131] 在上表2中，假设用户标识1为用户1的用户标识，则用户1对应的密钥即为密钥1；假设用户标识2为用户2的用户标识，则用户2对应的密钥即为密钥2；以此类推。

[0132] 下面以企业A开具给企业B的发票为例对本说明书进行描述。

[0133] 首先企业A和企业B可以分别通过其所使用的客户端发起注册请求。

[0134] 区块链中的节点设备在接收到该注册请求后，可以响应于该注册请求，调用部署在该区块链上的智能合约中的密钥分配逻辑，分别为企业A和企业B分配密钥。

[0135] 假设企业A的用户标识为税号A，为企业A分配的密钥为密钥A；企业B的用户标识为税号B，为企业B分配的密钥为密钥B，则部署在区块链上的智能合约中可以存储如下表3所示的用户标识和密钥的对应关系：

[0136]

税号A	密钥A
税号B	密钥B
……	……

[0137] 表3

[0138] 企业A在开具发票给企业B时，可以通过客户端发起针对该发票的创建请求。

[0139] 该区块链中的节点设备在接收到该创建请求后，可以响应于该创建请求，确定该发票的开票方为企业A(用户标识为税号A)，并确定该发票的受票方为企业B(用户标识为税号B)。

[0140] 在确定了该发票的开票方和受票方后，一方面，可以基于企业A(开票方)的税号A确定企业A对应的密钥A，并基于密钥A对该发票的明文数据进行加密处理，得到企业A对应的该发票的密文数据A；另一方面，可以基于企业B(受票方)的税号B确定企业B对应的密钥B，并基于密钥B对该发票的明文数据进行加密处理，得到企业B对应的该发票的密文数据B。

[0141] 后续,可以将该发票的密文数据(密文数据A和密文数据B),以及该发票的开票方和受票方的用户标识(税号A和税号B)以下表4所示的存储形式发布至该区块链中进行存储:

[0142]

密文数据A	税号A	密文数据B	税号B

[0143] 表4

[0144] 企业B在访问该发票时,可以通过客户端发起针对该发票的访问请求。其中,该访问请求中可以包括税号B。

[0145] 该区块链中的节点设备在接收到该访问请求后,可以响应于该访问请求,先获取该发票的开票方和受票方的用户标识,分别为税号A和税号B。后续,可以判断企业B的用户标识(税号B)与该发票的开票方和受票方的用户标识(税号A和税号B)是否匹配。

[0146] 由于企业B的用户标识即为该发票的受票方的用户标识,即企业B是该发票的受票方,因此可以确定企业B的用户标识与该发票的受票方的用户标识匹配,从而可以确定企业B具有该目标发票的访问权限。

[0147] 后续,可以基于企业B的税号B确定企业B对应的密钥B,并基于密钥B对该发票的密文数据进行解密处理,得到该发票的明文数据,并将该发票的明文数据返回给企业B所使用的客户端。

[0148] 在上述技术方案中,在用户需要访问被加密存储的区块链中的发票时,可以通过调用部署在该区块链上的智能合约中相应的逻辑,实现对该用户进行访问权限验证,并在确定该用户具有该发票的访问权限时,允许该用户访问该发票。采用这样的方式,可以保证在区块链上流转的发票的数据安全性,避免发票数据泄露而导致安全隐患。

[0149] 与前述基于区块链的发票访问方法的实施例相对应,本说明书还提供了基于区块链的发票访问装置的实施例。

[0150] 本说明书基于区块链的发票访问装置的实施例可以应用在电子设备上。装置实施例可以通过软件实现,也可以通过硬件或者软硬件结合的方式实现。以软件实现为例,作为一个逻辑意义上的装置,是通过其所在电子设备的处理器将非易失性存储器中对应的计算机程序指令读取到内存中运行形成的。从硬件层面而言,如图3所示,为本说明书基于区块链的发票访问装置所在电子设备的一种硬件结构图,除了图3所示的处理器、内存、网络接口、以及非易失性存储器之外,实施例中装置所在的电子设备通常根据该基于区块链的发票访问的实际功能,还可以包括其他硬件,对此不再赘述。

[0151] 请参考图4,图4是本说明书一示例性实施例示出的一种基于区块链的发票访问装置的框图。该装置40可以应用于图3所示的电子设备,包括:

[0152] 第一接收模块401,用于接收访问用户通过客户端发起的针对目标发票的访问请求;其中,所述目标发票被加密存储在所述区块链中;

[0153] 第一确定模块402,用于响应于所述访问请求,确定所述访问用户是否具有所述目标发票的访问权限;

[0154] 解密模块403,用于在所述访问用户具有所述目标发票的访问权限时,调用预设的智能合约中声明的解密逻辑,对所述区块链中存储的所述目标发票的密文数据进行解密处理,并将解密得到的所述目标发票的明文数据返回至所述客户端。

[0155] 在本实施例中，所述智能合约中还可以声明针对所述访问用户的访问权限验证逻辑；

[0156] 所述第一确定模块401具体可以用于：

[0157] 调用所述智能合约中声明的所述访问权限验证逻辑，确定所述访问用户是否具有所述目标发票的访问权限。

[0158] 在本实施例中，所述装置40还可以包括：

[0159] 第二接收模块404，用于接收创建用户通过客户端发起的针对所述目标发票的创建请求；

[0160] 第二确定模块405，用于响应于所述创建请求，确定所述目标发票的开票方和受票方；

[0161] 加密模块406，用于调用所述智能合约中声明的加密逻辑，基于所述开票方和受票方对应的密钥，分别对所述目标发票的明文数据进行加密处理，并将加密得到的所述目标发票的密文数据，以及所述目标发票的开票方和受票方的用户标识发布至所述区块链中进行存储。

[0162] 在本实施例中，所述加密模块406具体可以用于：

[0163] 基于所述开票方对应的密钥，对所述目标发票的明文数据进行加密处理，得到第一密文数据；

[0164] 基于所述受票方对应的密钥，对所述目标发票的明文数据进行加密处理，得到第二密文数据；

[0165] 将加密得到的所述目标发票的密文数据，以及所述目标发票的开票方和受票方的用户标识发布至所述区块链中进行存储，包括：

[0166] 将所述第一密文数据与所述开票方的用户标识的对应关系发布至所述区块链中进行存储；

[0167] 将所述第二密文数据与所述受票方的用户标识的对应关系发布至所述区块链中进行存储。

[0168] 在本实施例中，所述访问请求中可以包括所述访问用户的用户标识；

[0169] 所述第一确定模块401具体可以用于：

[0170] 获取所述目标发票的开票方和受票方的用户标识；

[0171] 判断所述访问用户的用户标识与所述开票方和受票方的用户标识是否匹配；

[0172] 如果所述访问用户的用户标识与所述开票方和受票方的用户标识匹配，则确定所述访问用户具有所述目标发票的访问权限。

[0173] 在本实施例中，所述解密模块403具体可以用于：

[0174] 基于所述访问用户对应的密钥，对所述区块链中存储的所述目标发票的密文数据进行解密处理。

[0175] 在本实施例中，所述智能合约中还可以声明密钥分配逻辑；

[0176] 所述装置40还可以包括：

[0177] 第三接收模块407，用于接收用户通过客户端发起的注册请求；

[0178] 注册模块408，用于响应于所述注册请求，调用所述智能合约中的所述密钥分配逻辑，将所述用户的用户标识和为所述用户分配的密钥的对应关系写入所述智能合约。

[0179] 在本实施例中，所述用户标识可以为纳税人识别号。

[0180] 上述装置中各个模块的功能和作用的实现过程具体详见上述方法中对应步骤的实现过程，在此不再赘述。

[0181] 对于装置实施例而言，由于其基本对应于方法实施例，所以相关之处参见方法实施例的部分说明即可。以上所描述的装置实施例仅仅是示意性的，其中所述作为分离部件说明的模块可以是或者也可以不是物理上分开的，作为模块显示的部件可以是或者也可以不是物理模块，即可以位于一个地方，或者也可以分布到多个网络模块上。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说明书方案的目的。本领域普通技术人员在不付出创造性劳动的情况下，即可以理解并实施。

[0182] 上述实施例阐明的系统、装置、模块或模块，具体可以由计算机芯片或实体实现，或者由具有某种功能的产品来实现。一种典型的实现设备为计算机，计算机的具体形式可以是个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件收发设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任意几种设备的组合。

[0183] 与上述基于区块链的发票访问方法实施例相对应，本说明书还提供了一种电子设备的实施例。该电子设备包括：处理器以及用于存储机器可执行指令的存储器；其中，处理器和存储器通常通过内部总线相互连接。在其他可能的实现方式中，所述设备还可能包括外部接口，以能够与其他设备或者部件进行通信。

[0184] 在本实施例中，通过读取并执行所述存储器存储的与基于区块链的发票访问的控制逻辑对应的机器可执行指令，所述处理器被促使：

[0185] 接收访问用户通过客户端发起的针对目标发票的访问请求；其中，所述目标发票被加密存储在所述区块链中；

[0186] 响应于所述访问请求，确定所述访问用户是否具有所述目标发票的访问权限；

[0187] 如果所述访问用户具有所述目标发票的访问权限，则调用预设的智能合约中声明的解密逻辑，对所述区块链中存储的所述目标发票的密文数据进行解密处理，并将解密得到的所述目标发票的明文数据返回至所述客户端。

[0188] 在本实施例中，所述智能合约中还可以声明针对所述访问用户的访问权限验证逻辑；

[0189] 通过读取并执行所述存储器存储的与基于区块链的发票访问的控制逻辑对应的机器可执行指令，所述处理器被促使：

[0190] 调用所述智能合约中声明的所述访问权限验证逻辑，确定所述访问用户是否具有所述目标发票的访问权限。

[0191] 在本实施例中，通过读取并执行所述存储器存储的与基于区块链的发票访问的控制逻辑对应的机器可执行指令，所述处理器还被促使：

[0192] 接收创建用户通过客户端发起的针对所述目标发票的创建请求；

[0193] 响应于所述创建请求，确定所述目标发票的开票方和受票方；

[0194] 调用所述智能合约中声明的加密逻辑，基于所述开票方和受票方对应的密钥，分别对所述目标发票的明文数据进行加密处理，并将加密得到的所述目标发票的密文数据，以及所述目标发票的开票方和受票方的用户标识发布至所述区块链中进行存储。

[0195] 在本实施例中，通过读取并执行所述存储器存储的与基于区块链的发票访问的控制逻辑对应的机器可执行指令，所述处理器被促使：

[0196] 基于所述开票方对应的密钥，对所述目标发票的明文数据进行加密处理，得到第一密文数据；

[0197] 基于所述受票方对应的密钥，对所述目标发票的明文数据进行加密处理，得到第二密文数据；

[0198] 将加密得到的所述目标发票的密文数据，以及所述目标发票的开票方和受票方的用户标识发布至所述区块链中进行存储，包括：

[0199] 将所述第一密文数据与所述开票方的用户标识的对应关系发布至所述区块链中进行存储；

[0200] 将所述第二密文数据与所述受票方的用户标识的对应关系发布至所述区块链中进行存储。

[0201] 在本实施例中，所述访问请求中可以包括所述访问用户的用户标识；

[0202] 通过读取并执行所述存储器存储的与基于区块链的发票访问的控制逻辑对应的机器可执行指令，所述处理器被促使：

[0203] 获取所述目标发票的开票方和受票方的用户标识；

[0204] 判断所述访问用户的用户标识与所述开票方和受票方的用户标识是否匹配；

[0205] 如果所述访问用户的用户标识与所述开票方和受票方的用户标识匹配，则确定所述访问用户具有所述目标发票的访问权限。

[0206] 通过读取并执行所述存储器存储的与基于区块链的发票访问的控制逻辑对应的机器可执行指令，所述处理器被促使：

[0207] 基于所述访问用户对应的密钥，对所述区块链中存储的所述目标发票的密文数据进行解密处理。

[0208] 在本实施例中，所述智能合约中还可以声明密钥分配逻辑；

[0209] 通过读取并执行所述存储器存储的与基于区块链的发票访问的控制逻辑对应的机器可执行指令，所述处理器还被促使：

[0210] 接收用户通过客户端发起的注册请求；

[0211] 响应于所述注册请求，调用所述智能合约中的所述密钥分配逻辑，将所述用户的用户标识和为所述用户分配的密钥的对应关系写入所述智能合约。

[0212] 在本实施例中，所述用户标识可以为纳税人识别号。

[0213] 本领域技术人员在考虑说明书及实践这里公开的发明后，将容易想到本说明书的其它实施方案。本说明书旨在涵盖本说明书的任何变型、用途或者适应性变化，这些变型、用途或者适应性变化遵循本说明书的一般性原理并包括本说明书未公开的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的，本说明书的真正范围和精神由下面的权利要求指出。

[0214] 应当理解的是，本说明书并不局限于上面已经描述并在附图中示出的精确结构，并且可以在不脱离其范围进行各种修改和改变。本说明书的范围仅由所附的权利要求来限制。

[0215] 以上所述仅为本说明书的较佳实施例而已，并不用以限制本说明书，凡在本说明

书的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本说明书保护的范围之内。

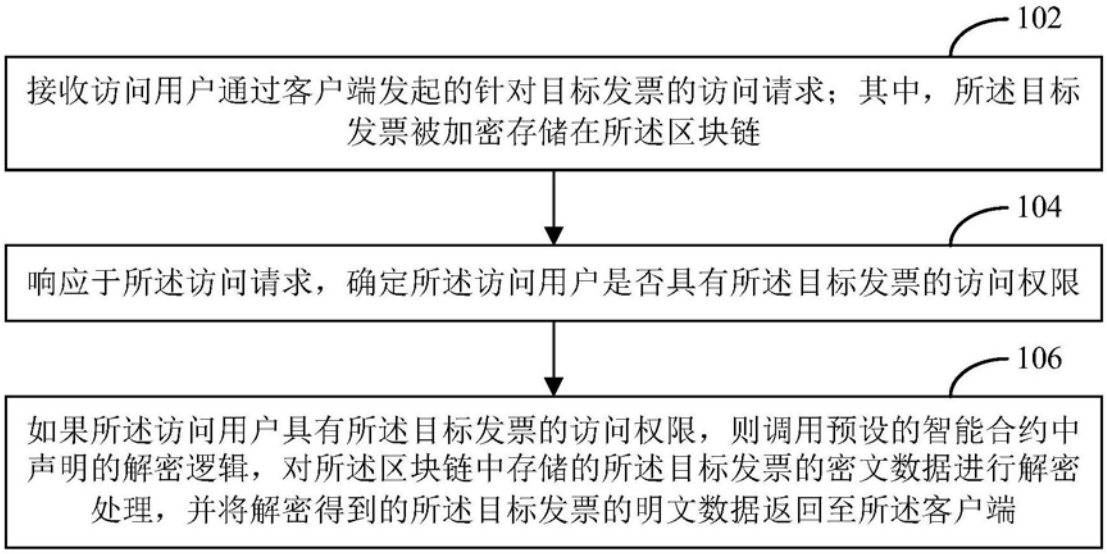

102
接收访问用户通过客户端发起的针对目标发票的访问请求；其中，所述目标发票被加密存储在所述区块链
104
响应于所述访问请求，确定所述访问用户是否具有所述目标发票的访问权限
106
如果所述访问用户具有所述目标发票的访问权限，则调用预设的智能合约中声明的解密逻辑，对所述区块链中存储的所述目标发票的密文数据进行解密处理，并将解密得到的所述目标发票的明文数据返回至所述客户端

图1

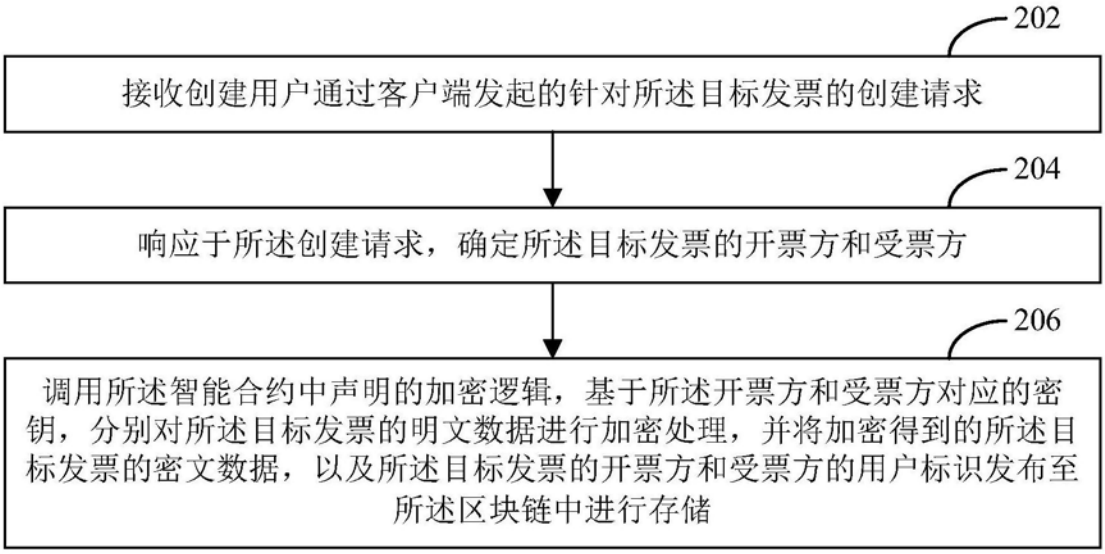

202
接收创建用户通过客户端发起的针对所述目标发票的创建请求
204
响应于所述创建请求，确定所述目标发票的开票方和受票方
206
调用所述智能合约中声明的加密逻辑，基于所述开票方和受票方对应的密钥，分别对所述目标发票的明文数据进行加密处理，并将加密得到的所述目标发票的密文数据，以及所述目标发票的开票方和受票方的用户标识发布至所述区块链中进行存储

图2

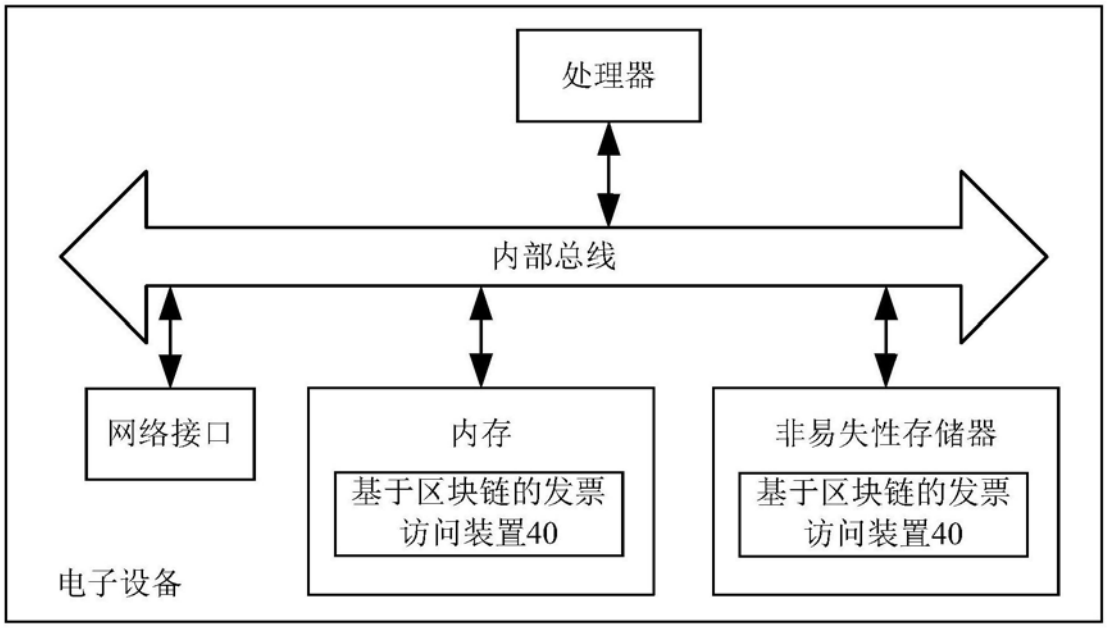

处理器
内部总线
网络接口
内存
基于区块链的发票访问装置40
非易失性存储器
基于区块链的发票访问装置40
电子设备

图3

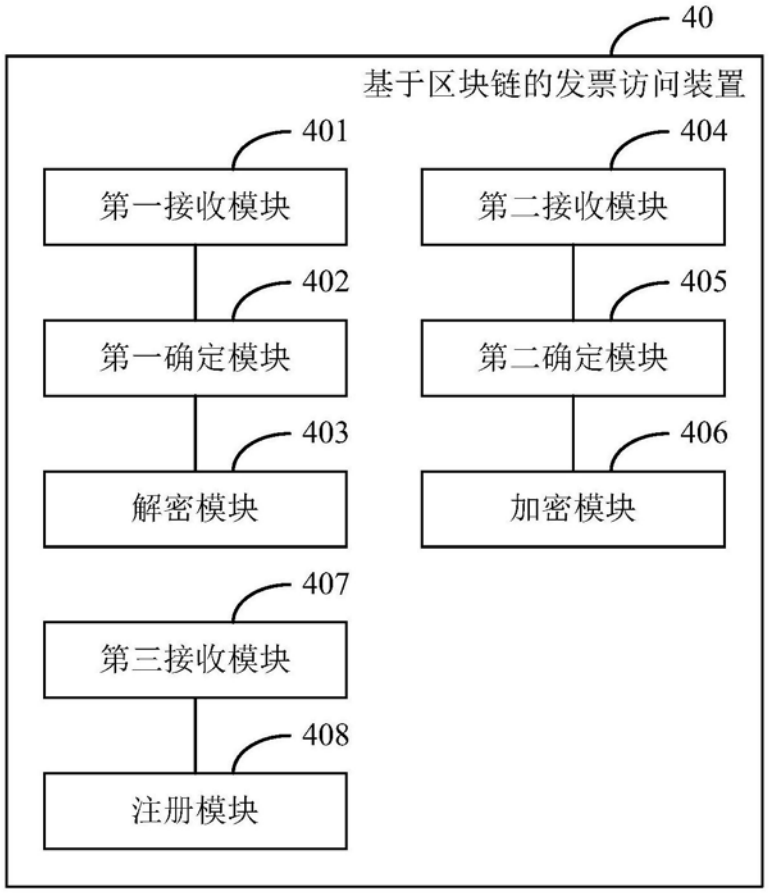

40
基于区块链的发票访问装置
401
第一接收模块
402
第一确定模块
403
解密模块
404
第二接收模块
405
第二确定模块
406
加密模块
407
第三接收模块
408
注册模块

图4