

数据共享方法、装置及系统、电子设备

技术领域

[01]本说明书一个或多个实施例涉及区块链技术领域，尤其涉及一种数据共享方法、装置及系统、电子设备。

5 背景技术

[02]在相关技术中，不同成员之间可以实现数据共享。比如，常见的数据共享模式为托管模式，即数据中心对各个成员的数据进行托管，而对于数据的后续处理完全依赖于数据中心。另一种常见的数据共享模式为聚合模式，即数据由不同成员各自控制、数据中心仅起到链接和撮合的功能，而由于数据中心有能力和机会留存被共享的数据，使得随着数据共享的不断进行，聚合模式会逐步发展为托管模式。

发明内容

[03]有鉴于此，本说明书一个或多个实施例提供一种数据共享方法、装置及系统、电子设备。

[04]为实现上述目的，本说明书一个或多个实施例提供技术方案如下：

15 [05]根据本说明书一个或多个实施例的第一方面，提出了一种数据共享系统，包括：

[06]成员，每一成员分别维护有可共享的私有数据，并为所述私有数据生成相应的密文索引信息，所述密文索引信息包含对应的私有数据的密文索引和提供该私有数据的成员的信息；

20 [07]共享平台，所述共享平台分别连接至每一成员，并将每一成员生成的密文索引信息记录于索引区块链，以在所有成员之间进行共享；所述共享平台将数据请求方成员发起的数据获取请求转发至数据提供方成员，所述数据获取请求包含目标数据的密文索引，且所述共享平台还将所述数据提供方成员返回的所述目标数据转发至所述数据请求方成员，其中所述目标数据由所述数据请求方成员的身份公钥进行加密。

25 [08]根据本说明书一个或多个实施例的第二方面，提出了一种数据共享方法，应用于作为数据请求方的成员，所述方法包括：

[09]确定索引区块链中记录的对应于目标数据的索引信息集合，所述索引信息集合包含

所述目标数据的密文索引和所述目标数据的数据提供方的成员信息,所述索引信息集合由所述数据提供方共享至所述索引区块链;

[10]通过共享平台向所述数据提供方发起数据获取请求,所述数据获取请求包含所述目标数据的密文索引;

- 5 [11]接收所述共享平台返回的响应数据,所述响应数据由所述数据请求方的身份公钥进行加密。

[12]根据本说明书一个或多个实施例的第三方面,提出了一种数据共享方法,应用于作为数据提供方的成员,所述方法包括:

- [13]将对应于目标数据的索引信息集合共享至索引区块链,所述索引信息集合包含所述
10 目标数据的密文索引和所述数据提供方的成员信息;

[14]接收数据请求方通过共享平台发起的数据获取请求,所述数据获取请求包含所述目标数据的密文索引;

[15]通过所述共享平台向所述数据请求方返回响应数据,所述响应数据由所述数据请求方的身份公钥进行加密。

- 15 [16]根据本说明书一个或多个实施例的第四方面,提出了一种数据共享方法,应用于共享平台,所述方法包括:

[17]将对应于目标数据的索引信息集合发布至索引区块链,所述索引信息集合包含所述目标数据的密文索引和所述目标数据的数据提供方的成员信息,所述索引信息集合由所述数据提供方提交至所述共享平台;

- 20 [18]将数据请求方发起的数据获取请求转发至所述数据提供方,所述数据获取请求包含所述目标数据的密文索引;

[19]将所述数据提供方提供的响应数据返回至所述数据请求方,所述响应数据由所述数据请求方的身份公钥进行加密。

- [20]根据本说明书一个或多个实施例的第五方面,提出了一种数据共享装置,应用于作
25 为数据请求方的成员,所述装置包括:

[21]确定单元,确定索引区块链中记录的对应于目标数据的索引信息集合,所述索引信息集合包含所述目标数据的密文索引和所述目标数据的数据提供方的成员信息,所述索引信息集合由所述数据提供方共享至所述索引区块链;

- [22]请求单元，通过共享平台向所述数据提供方发起数据获取请求，所述数据获取请求包含所述目标数据的密文索引；
- [23]接收单元，接收所述共享平台返回的响应数据，所述响应数据由所述数据请求方的身份公钥进行加密。
- 5 [24]根据本说明书一个或多个实施例的第六方面，提出了一种数据共享装置，应用于作为数据提供方的成员，所述装置包括：
- [25]共享单元，将对应于目标数据的索引信息集合共享至索引区块链，所述索引信息集合包含所述目标数据的密文索引和所述数据提供方的成员信息；
- [26]接收单元，接收数据请求方通过共享平台发起的数据获取请求，所述数据获取请求
- 10 包含所述目标数据的密文索引；
- [27]返回单元，通过所述共享平台向所述数据请求方返回响应数据，所述响应数据由所述数据请求方的身份公钥进行加密。
- [28]根据本说明书一个或多个实施例的第七方面，提出了一种数据共享装置，应用于共享平台，所述装置包括：
- 15 [29]第一发布单元，将对应于目标数据的索引信息集合发布至索引区块链，所述索引信息集合包含所述目标数据的密文索引和所述目标数据的数据提供方的成员信息，所述索引信息集合由所述数据提供方提交至所述共享平台；
- [30]转发单元，将数据请求方发起的数据获取请求转发至所述数据提供方，所述数据获取请求包含所述目标数据的密文索引；
- 20 [31]返回单元，将所述数据提供方提供的响应数据返回至所述数据请求方，所述响应数据由所述数据请求方的身份公钥进行加密。
- [32]根据本说明书一个或多个实施例的第八方面，提出了一种电子设备，包括：
- [33]处理器；
- [34]用于存储处理器可执行指令的存储器；
- 25 [35]其中，所述处理器通过运行所述可执行指令以实现如上述第一方面所述的方法。
- [36]根据本说明书一个或多个实施例的第九方面，提出了一种电子设备，包括：
- [37]处理器；

[38]用于存储处理器可执行指令的存储器;

[39]其中, 所述处理器通过运行所述可执行指令以实现如上述第二方面所述的方法。

[40]根据本说明书一个或多个实施例的第十方面, 提出了一种电子设备, 包括:

[41]处理器;

5 [42]用于存储处理器可执行指令的存储器;

[43]其中, 所述处理器通过运行所述可执行指令以实现如上述第三方面所述的方法。

附图说明

[44]图 1 是一示例性实施例提供的一种数据共享方法的流程图。

[45]图 2 是一示例性实施例提供的另一种数据共享方法的流程图。

10 [46]图 3 是一示例性实施例提供的又一种数据共享方法的流程图。

[47]图 4 是一示例性实施例提供的一种数据共享系统的结构示意图。

[48]图 5 是一示例性实施例提供的一种数据共享过程的交互示意图。

[49]图 6 是一示例性实施例提供的一种身份认证的交互示意图。

[50]图 7 是一示例性实施例提供的一种记录申请包的结构示意图。

15 [51]图 8 是一示例性实施例提供的一种数据获取请求包的结构示意图。

[52]图 9 是一示例性实施例提供的一种响应包的结构示意图。

[53]图 10 是一示例性实施例提供的一种投诉请求包的结构示意图。

[54]图 11 是一示例性实施例提供的一种设备的结构示意图。

[55]图 12 是一示例性实施例提供的一种数据共享装置的框图。

20 [56]图 13 是一示例性实施例提供的另一种设备的结构示意图。

[57]图 14 是一示例性实施例提供的另一种数据共享装置的框图。

[58]图 15 是一示例性实施例提供的又一种设备的结构示意图。

[59]图 16 是一示例性实施例提供的又一种数据共享装置的框图。

具体实施方式

[60]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发明一个或多个实施例相一致的所有实施方式。

- 5 相反，它们仅是与如所附权利要求书中所详述的、本发明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。

[61]需要说明的是：在其他实施例中并不一定按照本发明示出和描述的顺序来执行相应方法的步骤。在一些其他实施例中，其方法所包括的步骤可以比本发明所描述的更多或更少。此外，本发明中所描述的单个步骤，在其他实施例中可能被分解为多个步骤进行描述；而本发明中所描述的多个步骤，在其他实施例中也可能被合并为单个步骤进行描述。

[62]图1是一示例性实施例提供的一种数据共享方法的流程图。如图1所示，该方法应用于作为数据请求方的成员，可以包括以下步骤：

- [63]步骤102，确定索引区块链中记录的对应于目标数据的索引信息集合，所述索引信息集合包含所述目标数据的密文索引和所述目标数据的数据提供方的成员信息，所述索引信息集合由所述数据提供方共享至所述索引区块链。

[64]在一实施例中，多个成员之间可以基于本发明的技术方案实现数据共享，在共享过程中存在不同角色：若由成员A向用户B发起数据获取请求，而用户B将自身维护的私有数据返回至成员A，则成员A扮演了数据请求方的角色、用户B扮演了数据提供方的角色。每一成员均可能扮演数据请求方或数据提供方的角色，本发明并不对此进行限制。

[65]在一实施例中，对于各个成员所维护的私有数据而言，这些私有数据对应的索引信息集合可以被发布至索引区块链，并记录至索引区块链的所有区块链节点分别维护的、内容统一的索引区块链账本中，使得每一成员均可以基于索引区块链账本获知各个成员所维护的私有数据对应的索引信息集合。

[66]在一实施例中，共享平台可以被配置为所述索引区块链的节点，各个成员可以为自身所维护的私有数据生成索引信息集合，并将索引信息集合发送至共享平台，以由共享平台提交至索引区块链。而各个成员可以通过共享平台或其他区块链节点对索引区块链账本进行查询，或者各个成员可以从共享平台或其他区块链节点处下载索引区块链账本

的账本数据，以对自身发送给共享平台的索引信息集合进行查询，以确定共享平台是否已经将该索引信息集合发布至索引区块链。

5 [67]在一实施例中，各个成员被配置为索引区块链的区块链节点，使得每一成员可以为自身所维护的私有数据生成索引信息集合，并通过向索引区块链中提交包含索引信息集合的区块链交易，从而将索引信息集合发布至索引区块链，无需依赖于共享平台。

10 [68]在一实施例中，共享平台可以被配置为所述索引区块链的节点，即该共享平台维护有索引区块链对应的索引区块链账本。相应地，作为数据请求方的成员可以根据已知的目标数据的特定信息（比如当目标数据为交易记录时，该特定信息可以包括交易记录对应的交易用户 ID 等），生成相应的密文索引（比如特定信息的哈希值），并向所述共享平台发起查询请求，所述查询请求中包含所述密文索引，以指示所述共享平台从所述索引区块链中查询包含所述密文索引的索引信息集合，即由共享平台根据密文索引对索引区块链账本进行检索、查询到该密文索引对应的索引信息集合。或者，作为数据请求方的成员可以请求下载所述共享平台维护的所述索引区块链的账本数据（即索引区块链账本的数据），并由该数据请求方自身根据密文索引对账本数据进行检索，以查询出包
15 含所述密文索引的索引信息集合。

[69]在一实施例中，所述数据请求方被配置为所述索引区块链的节点。相应地，作为数据请求方的成员可以根据已知的所述目标数据的特定信息，生成相应的密文索引，并根据所述数据请求方维护的所述索引区块链的账本数据，查询出包含所述密文索引的索引信息集合，无需依赖于共享平台。

20 [70]在一实施例中，由于私有数据由各个成员进行维护，而共享平台仅能够接触到私有数据对应的索引信息（包含于上述的索引信息集合中），可以避免共享平台获取私有数据并违规外泄私有数据。同时，通过采用索引区块链来记录索引信息集合，可以利用区块链的链式数据结构，确保已经上链的索引信息集合无法被随意修改，并且可供共享平台和各个成员进行查询、验证，具有极高的可靠性。此外，由于索引区块链上记录的索引信息集合中，与私有数据相关的索引信息为密文索引、呈现为密文形式，因而不会向
25 共享平台透露出数据提供方实际持有的私有数据的内容，也不会暴露数据请求方请求了何种数据，具有极高的私密性。

[71]步骤 104，通过共享平台向所述数据提供方发起数据获取请求，所述数据获取请求包含所述目标数据的密文索引。

[72]在一实施例中，通过确定出索引信息集合，使得数据请求方可以获知该索引信息集合中包含的数据提供方的信息，即确定出目标数据对应的数据提供方，从而向共享平台发起针对该数据提供方的数据获取请求。

[73]在一实施例中，数据获取请求还包含：所述数据请求方的身份公钥、通过所述数据请求方的身份私钥生成的数据请求方签名，使得数据提供方在获得共享平台转发的该数据获取请求后，可以从数据获取请求中提取出身份公钥，以针对数据请求方签名进行验证，若验证成功则确定该数据获取请求确实来自于该数据请求方。当然，在一些情况下，数据获取请求中可以不包含数据请求方的身份公钥，比如可以包含唯一对应于该数据请求方的身份标识，而数据提供方可以据此选取预先获得的该数据请求方的身份公钥，以针对数据请求方签名进行验证。

[74]步骤 106，接收所述共享平台返回的响应数据，所述响应数据由所述数据请求方的身份公钥进行加密。

[75]在一实施例中，数据提供方根据数据获取请求中包含的密文索引，以及自身维护的密文索引与明文索引之间的映射关系，确定出明文索引，并基于该明文索引查询出相应的私有数据，以作为上述的响应数据而返回至共享平台、由共享平台转发至数据请求方。当然，数据提供方也可以维护有密文索引与私有数据之间的映射关系，从而直接根据密文索引查询到对应的私有数据。

[76]在一实施例中，通过采用数据请求方的身份公钥对响应数据进行加密，使得该响应数据只有数据请求方可以通过自身的身份私钥进行解密，那么即便由共享平台对该响应数据进行转发，该共享平台也只能够获得加密状态的响应数据，从而杜绝了共享平台沉淀与外泄私有数据的可能性。

[77]在一实施例中，所述响应数据中还包含：通过所述数据提供方的身份私钥生成的数据提供方签名，使得数据请求方可以根据该数据提供方的身份公钥进行验证，若验证通过则确定该响应数据确实来自于所述数据提供方。

[78]在一实施例中，所述索引信息集合中包含所述目标数据的哈希值；数据请求方可以将所述响应数据对应的解密后数据进行哈希计算，并与索引信息集合中的哈希值进行比较，当计算得到的哈希值与所述索引信息集合中的哈希值一致时，可以确定所述解密后数据为所述目标数据，表明数据提供方确实拥有相关数据并且没有无意或刻意提供错误的数据，且数据传输过程中没有发生数据损坏或数据替换，也可以表明数据提供方提供

至索引区块链的索引信息集合与其实际拥有的私有数据之间内容相符、不存在欺骗行为。

- [79]在一实施例中,数据请求方可以向所述共享平台发起针对所述目标数据的投诉请求,所述投诉请求中包含投诉理由和相关数据;其中,当所述投诉理由被所述共享平台或所述共享平台在所述索引区块链中调用的智能合约基于所述相关数据而验证为成立时,所述索引信息集合在所述索引区块链中被添加无效标识,而具有无效标识的索引信息集合无法被用于数据共享。其中,根据投诉理由的不同,投诉请求所包含的相关数据的类型也可能存在差异,需要根据实际情况而确定。例如,当投诉理由为数据重复时,相关数据可以包括数据请求方持有数据的信息和被诉数据的信息,使得两者被确认为一致且数据请求方所持有数据的索引信息集合在索引区块链上的区块高度相对较小(即更早提交至索引区块链)时,可以判定为投诉理由成立。再例如,当投诉理由为数据不符时,相关数据可以包括数据请求方获得的目标数据、相应的索引信息集合、数据请求方从数据提供方处获得该目标数据的历史记录等,使得共享平台可以根据历史记录确定该目标数据来自数据提供方,以及共享平台可以计算目标数据的哈希值、与索引信息集合中包含的哈希值进行比较,从而该比较结果为不一致时,判定为投诉理由成立。
- [80]在一实施例中,数据请求方可以向所述索引区块链提交投诉类型的交易,以调取用于处理投诉的智能合约,其中所述交易包含投诉理由和相关数据;其中,所述智能合约被用于根据所述相关数据验证所述投诉理由,并在所述投诉理由被验证为成立时,在所述索引区块链中为所述索引信息集合添加无效标识。由于智能合约被记录于索引区块链中,使得智能合约的处理逻辑公开且不可篡改,同时智能合约为自动执行、避免外部因素的干扰,可以确保智能合约对投诉理由的验证结果公正可靠。
- [81]在一实施例中,数据请求方可以将自身与所述数据提供方之间的数据共享事件发布至交易区块链,其中所述数据请求方被配置为所述交易区块链的节点。在另一实施例中,数据请求方可以将所述数据共享事件发送至所述共享平台,以由所述共享平台发布至所述交易区块链,其中所述共享平台被配置为所述交易区块链的节点。其中,交易区块链区别于上述的索引区块链,该交易区块链用于记录各个成员之间的数据共享事件,以便后续查询与验证。而通过采用相互独立的索引区块链与交易区块链,可以将索引信息集合的数据与数据共享事件的数据相互分离,尤其是索引区块链需要频繁实施索引查询操作,这样有助于提升对索引信息集合的查询效率。当然,也可以仅采用单一的区块链,并将索引信息集合与数据共享事件均记录至该区块链中,本说明书并不对此进行限制。
- [82]图2是一示例性实施例提供的另一种数据共享方法的流程图。如图2所示,该方法

应用于作为数据提供方的成员，可以包括以下步骤：

[83] 步骤 202，将对应于目标数据的索引信息集合共享至索引区块链，所述索引信息集合包含所述目标数据的密文索引和所述数据提供方的成员信息。

5 [84] 在一实施例中，多个成员之间可以基于本说明书的技术方案实现数据共享，在共享过程中存在不同角色：若由成员 A 向用户 B 发起数据获取请求，而用户 B 将自身维护的私有数据返回至成员 A，则成员 A 扮演了数据请求方的角色、用户 B 扮演了数据提供方的角色。每一成员均可能扮演数据请求方或数据提供方的角色，本说明书并不对此进行限制。

10 [85] 在一实施例中，对于各个成员所维护的私有数据而言，这些私有数据对应的索引信息集合可以被发布至索引区块链，并记录至索引区块链的所有区块链节点分别维护的、内容统一的索引区块链账本中，使得每一成员均可以基于索引区块链账本获知各个成员所维护的私有数据对应的索引信息集合。

15 [86] 在一实施例中，共享平台可以被配置为所述索引区块链的节点，各个成员可以为自身所维护的私有数据生成索引信息集合，并将索引信息集合发送至共享平台，以由共享平台提交至索引区块链。而各个成员可以通过共享平台或其他区块链节点对索引区块链账本进行查询，或者各个成员可以从共享平台或其他区块链节点处下载索引区块链账本的账本数据，以对自身发送给共享平台的索引信息集合进行查询，以确定共享平台是否已经将该索引信息集合发布至索引区块链。

20 [87] 在一实施例中，各个成员被配置为索引区块链的区块链节点，使得每一成员可以为自身所维护的私有数据生成索引信息集合，并通过向索引区块链中提交包含索引信息集合的区块链交易，从而将索引信息集合发布至索引区块链，无需依赖于共享平台。

25 [88] 在一实施例中，共享平台可以被配置为所述索引区块链的节点，即该共享平台维护有索引区块链对应的索引区块链账本。相应地，作为数据请求方的成员可以根据已知的目标数据的特定信息（比如当目标数据为交易记录时，该特定信息可以包括交易记录对应的交易用户 ID 等），生成相应的密文索引（比如特定信息的哈希值），并向所述共享平台发起查询请求，所述查询请求中包含所述密文索引，以指示所述共享平台从所述索引区块链中查询包含所述密文索引的索引信息集合，即由共享平台根据密文索引对索引区块链账本进行检索、查询到该密文索引对应的索引信息集合。或者，作为数据请求方的成员可以请求下载所述共享平台维护的所述索引区块链的账本数据（即索引区块链

账本的数据)，并由该数据请求方自身根据密文索引对账本数据进行检索，以查询出包含所述密文索引的索引信息集合。

[89]在一实施例中，所述数据请求方被配置为所述索引区块链的节点。相应地，作为数据请求方的成员可以根据已知的所述目标数据的特定信息，生成相应的密文索引，并根据所述数据请求方维护的所述索引区块链的账本数据，查询出包含所述密文索引的索引信息集合，无需依赖于共享平台。

[90]在一实施例中，由于私有数据由各个成员进行维护，而共享平台仅能够接触到私有数据对应的索引信息（包含于上述的索引信息集合中），可以避免共享平台获取私有数据并违规外泄私有数据。同时，通过采用索引区块链来记录索引信息集合，可以利用区块链的链式数据结构，确保已经上链的索引信息集合无法被随意修改，并且可供共享平台和各个成员进行查询、验证，具有极高的可靠性。此外，由于索引区块链上记录的索引信息集合中，与私有数据相关的索引信息为密文索引、呈现为密文形式，因而不会向共享平台透露出数据提供方实际持有的私有数据的内容，也不会暴露数据请求方请求了何种数据，具有极高的私密性。

[91]步骤 204，接收数据请求方通过共享平台发起的数据获取请求，所述数据获取请求包含所述目标数据的密文索引。

[92]在一实施例中，通过确定出索引信息集合，使得数据请求方可以获知该索引信息集合中包含的数据提供方的信息，即确定出目标数据对应的数据提供方，从而向共享平台发起针对该数据提供方的数据获取请求。

[93]在一实施例中，数据获取请求还包含：所述数据请求方的身份公钥、通过所述数据请求方的身份私钥生成的数据请求方签名，使得数据提供方在获得共享平台转发的该数据获取请求后，可以从数据获取请求中提取出身份公钥，以针对数据请求方签名进行验证，若验证成功则确定该数据获取请求确实来自于该数据请求方。当然，在一些情况下，数据获取请求中可以不包含数据请求方的身份公钥，比如可以包含唯一对应于该数据请求方的身份标识，而数据提供方可以据此选取预先获得的该数据请求方的身份公钥，以针对数据请求方签名进行验证。

[94]步骤 206，通过所述共享平台向所述数据请求方返回响应数据，所述响应数据由所述数据请求方的身份公钥进行加密。

[95]在一实施例中，数据提供方根据数据获取请求中包含的密文索引，以及自身维护的

密文索引与明文索引之间的映射关系，确定出明文索引，并基于该明文索引查询出相应的私有数据，以作为上述的响应数据而返回至共享平台、由共享平台转发至数据请求方。当然，数据提供方也可以维护有密文索引与私有数据之间的映射关系，从而直接根据密文索引查询到对应的私有数据。

- 5 [96]在一实施例中，通过采用数据请求方的身份公钥对响应数据进行加密，使得该响应数据只有数据请求方可以通过自身的身份私钥进行解密，那么即便由共享平台对该响应数据进行转发，该共享平台也只能够获得加密状态的响应数据，从而杜绝了共享平台沉淀与外泄私有数据的可能性。

- 10 [97]在一实施例中，所述响应数据中还包含：通过所述数据提供方的身份私钥生成的数据提供方签名，使得数据请求方可以根据该数据提供方的身份公钥进行验证，若验证通过则确定该响应数据确实来自于所述数据提供方。

- 15 [98]在一实施例中，所述索引信息集合中包含所述目标数据的哈希值；数据请求方可以将所述响应数据对应的解密后数据进行哈希计算，并与索引信息集合中的哈希值进行比较，当计算得到的哈希值与所述索引信息集合中的哈希值一致时，可以确定所述解密后数据为所述目标数据，表明数据提供方确实拥有相关数据并且没有无意或刻意提供错误的
- 数据，且数据传输过程中没有发生数据损坏或数据替换，也可以表明数据提供方提供至索引区块链的索引信息集合与其实际拥有的私有数据之间内容相符、不存在欺骗行为。

- 20 [99]在一实施例中，数据提供方可以将自身与所述数据请求方之间的数据共享事件发布至交易区块链，其中所述数据提供方被配置为所述交易区块链的节点。在另一实施例中，数据提供方可以将所述数据共享事件发送至所述共享平台，以由所述共享平台发布至所述交易区块链，其中所述共享平台被配置为所述交易区块链的节点。其中，交易区块链区别于上述的索引区块链，该交易区块链用于记录各个成员之间的数据共享事件，以便后续查询与验证。而通过采用相互独立的索引区块链与交易区块链，可以将索引信息集合的数据与数据共享事件的数据相互分离，尤其是索引区块链需要频繁实施索引查询操作，这样有助于提升对索引信息集合的查询效率。当然，也可以仅采用单一的区块链，并将索引信息集合与数据共享事件均记录至该区块链中，本说明书并不对此进行限制。
- 25

[100] 图3是一示例性实施例提供的又一种数据共享方法的流程图。如图3所示，该方法应用于共享平台，可以包括以下步骤：

[101] 步骤302，将对应于目标数据的索引信息集合发布至索引区块链，所述索引信息

集合包含所述目标数据的密文索引和所述目标数据的数据提供方的成员信息，所述索引信息集合由所述数据提供方提交至所述共享平台。

[102] 在一实施例中，多个成员之间可以基于本说明书的技术方案实现数据共享，在共享过程中存在不同角色：若由成员 A 向用户 B 发起数据获取请求，而用户 B 将自身维护的私有数据返回至成员 A，则成员 A 扮演了数据请求方的角色、用户 B 扮演了数据提供方的角色。每一成员均可能扮演数据请求方或数据提供方的角色，本说明书并不对此进行限制。

[103] 在一实施例中，对于各个成员所维护的私有数据而言，这些私有数据对应的索引信息集合可以被发布至索引区块链，并记录至索引区块链的所有区块链节点分别维护的、内容统一的索引区块链账本中，使得每一成员均可以基于索引区块链账本获知各个成员所维护的私有数据对应的索引信息集合。

[104] 在一实施例中，共享平台可以被配置为所述索引区块链的节点，各个成员可以为自身所维护的私有数据生成索引信息集合，并将索引信息集合发送至共享平台，以由共享平台提交至索引区块链。而各个成员可以通过共享平台或其他区块链节点对索引区块链账本进行查询，或者各个成员可以从共享平台或其他区块链节点处下载索引区块链账本的账本数据，以对自身发送给共享平台的索引信息集合进行查询，以确定共享平台是否已经将该索引信息集合发布至索引区块链。

[105] 在一实施例中，各个成员被配置为索引区块链的区块链节点，使得每一成员可以为自身所维护的私有数据生成索引信息集合，并通过向索引区块链中提交包含索引信息集合的区块链交易，从而将索引信息集合发布至索引区块链，无需依赖于共享平台。

[106] 在一实施例中，共享平台可以被配置为所述索引区块链的节点，即该共享平台维护有索引区块链对应的索引区块链账本。相应地，作为数据请求方的成员可以根据已知的目标数据的特定信息（比如当目标数据为交易记录时，该特定信息可以包括交易记录对应的交易用户 ID 等），生成相应的密文索引（比如特定信息的哈希值），并向所述共享平台发起查询请求，所述查询请求中包含所述密文索引，以指示所述共享平台从所述索引区块链中查询包含所述密文索引的索引信息集合，即由共享平台根据密文索引对索引区块链账本进行检索、查询到该密文索引对应的索引信息集合。或者，作为数据请求方的成员可以请求下载所述共享平台维护的所述索引区块链的账本数据（即索引区块链账本的数据），并由该数据请求方自身根据密文索引对账本数据进行检索，以查询出包含所述密文索引的索引信息集合。

[107] 在一实施例中，所述数据请求方被配置为所述索引区块链的节点。相应地，作为数据请求方的成员可以根据已知的所述目标数据的特定信息，生成相应的密文索引，并根据所述数据请求方维护的所述索引区块链的账本数据，查询出包含所述密文索引的索引信息集合，无需依赖于共享平台。

- 5 [108] 在一实施例中，由于私有数据由各个成员进行维护，而共享平台仅能够接触到私有数据对应的索引信息（包含于上述的索引信息集合中），可以避免共享平台获取私有数据并违规外泄私有数据。同时，通过采用索引区块链来记录索引信息集合，可以利用区块链的链式数据结构，确保已经上链的索引信息集合无法被随意修改，并且可供共享平台和各个成员进行查询、验证，具有极高的可靠性。此外，由于索引区块链上记录的索引信息集合中，与私有数据相关的索引信息为密文索引、呈现为密文形式，因而不会向共享平台透露出数据提供方实际持有的私有数据的内容，也不会暴露数据请求方请求了何种数据，具有极高的私密性。

[109] 步骤 304，将数据请求方发起的数据获取请求转发至所述数据提供方，所述数据获取请求包含所述目标数据的密文索引。

- 15 [110] 在一实施例中，通过确定出索引信息集合，使得数据请求方可以获知该索引信息集合中包含的数据提供方的信息，即确定出目标数据对应的数据提供方，从而向共享平台发起针对该数据提供方的数据获取请求。

- [111] 在一实施例中，数据获取请求还包含：所述数据请求方的身份公钥、通过所述数据请求方的身份私钥生成的数据请求方签名，使得数据提供方在获得共享平台转发的该数据获取请求后，可以从数据获取请求中提取出身份公钥，以针对数据请求方签名进行验证，若验证成功则确定该数据获取请求确实来自于该数据请求方。当然，在一些情况下，数据获取请求中可以不包含数据请求方的身份公钥，比如可以包含唯一对应于该数据请求方的身份标识，而数据提供方可以据此选取预先获得的该数据请求方的身份公钥，以针对数据请求方签名进行验证。

- 25 [112] 步骤 306，将所述数据提供方提供的响应数据返回至所述数据请求方，所述响应数据由所述数据请求方的身份公钥进行加密。

[113] 在一实施例中，数据提供方根据数据获取请求中包含的密文索引，以及自身维护的密文索引与明文索引之间的映射关系，确定出明文索引，并基于该明文索引查询出相应的私有数据，以作为上述的响应数据而返回至共享平台、由共享平台转发至数据请

求方。当然，数据提供方也可以维护有密文索引与私有数据之间的映射关系，从而直接根据密文索引查询到对应的私有数据。

[114] 在一实施例中，通过采用数据请求方的身份公钥对响应数据进行加密，使得该响应数据只有数据请求方可以通过自身的身份私钥进行解密，那么即便由共享平台对该响应数据进行转发，该共享平台也只能够获得加密状态的响应数据，从而杜绝了共享平台沉淀与外泄私有数据的可能性。

[115] 在一实施例中，所述响应数据中还包含：通过所述数据提供方的身份私钥生成的数据提供方签名，使得数据请求方可以根据该数据提供方的身份公钥进行验证，若验证通过则确定该响应数据确实来自于所述数据提供方。

10 [116] 在一实施例中，所述索引信息集合中包含所述目标数据的哈希值；数据请求方可以将所述响应数据对应的解密后数据进行哈希计算，并与索引信息集合中的哈希值进行比较，当计算得到的哈希值与所述索引信息集合中的哈希值一致时，可以确定所述解密后数据为所述目标数据，表明数据提供方确实拥有相关数据并且没有无意或刻意提供错误的数
15 据，且数据传输过程中没有发生数据损坏或数据替换，也可以表明数据提供方提供至索引区块链的索引信息集合与其实实际拥有的私有数据之间内容相符、不存在欺骗行为。

[117] 在一实施例中，共享平台可以接收所述数据请求方向所述共享平台发起针对所述目标数据的投诉请求，所述投诉请求中包含投诉理由和相关数据；当基于所述相关数据验证所述投诉理由成立时，在所述索引区块链中为所述索引信息集合添加无效标识。
20 其中，根据投诉理由的不同，投诉请求所包含的相关数据的类型也可能存在差异，需要根据实际情况而确定。例如，当投诉理由为数据重复时，相关数据可以包括数据请求方持有数据的信息和被告数据的信息，使得两者被确认为一致且数据请求方所持有数据的索引信息集合在索引区块链上的区块高度相对较小（即更早提交至索引区块链）时，可以判定为投诉理由成立。再例如，当投诉理由为数据不符时，相关数据可以包括数据请求方获得的
25 目标数据、相应的索引信息集合、数据请求方从数据提供方处获得该目标数据的历史记录等，使得共享平台可以根据历史记录确定该目标数据来自数据提供方，以及共享平台可以计算目标数据的哈希值、与索引信息集合中包含的哈希值进行比较，从而该比较结果为不一致时，判定为投诉理由成立。

[118] 在一实施例中，共享平台可以确定所述数据请求方与所述数据提供方之间的数据共享事件，并将所述数据共享事件发布至所述交易区块链，其中所述共享平台被配置

30

为所述交易区块链的节点。其中，交易区块链区别于上述的索引区块链，该交易区块链用于记录各个成员之间的数据共享事件，以便后续查询与验证。而通过采用相互独立的索引区块链与交易区块链，可以将索引信息集合的数据与数据共享事件的数据相互分离，尤其是索引区块链需要频繁实施索引查询操作，这样有助于提升对索引信息集合的查询效率。当然，也可以仅采用单一的区块链，并将索引信息集合与数据共享事件均记录至该区块链中，本说明书并不对此进行限制。

[119] 需要说明的是：在本说明书中所描述的交易（transfer），是指用户通过区块链的客户端创建，并需要最终发布至区块链的分布式数据库中的一笔数据。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，数据共享业务、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。

[120] 为了便于理解，以数据共享系统为例，对本说明书一个或多个实施例的技术方案进行说明。图4是一示例性实施例提供的一种数据共享系统的结构示意图。如图4所示，该数据共享系统可以包括：共享平台和若干成员，比如图4中示出了成员1~成员6，每一成员分别维护有可共享的私有数据，共享平台分别连接至每一成员，从而实现各个成员之间的数据共享。图5是一示例性实施例提供的一种数据共享过程的交互示意图；如图5所示，该数据共享过程可以包括以下步骤：

[121] 步骤501a，机构1通过在共享平台进行身份认证，加入为共享平台相关联的成员1。

[122] 在一实施例中，数据共享系统中的成员可以包括管理数据的机构；或者，数据共享系统中的成员还可以包括个人或除机构之外的其他类型的组织等，本说明书并不对此进行限制。

[123] 以机构1为例，图6是一示例性实施例提供的一种身份认证的交互示意图；如图6所示，在步骤601中由机构1向共享平台发送成员加入申请，该成员加入申请中可以包含机构1的身份证明信息（比如营业执照、法人信息、资质证明等，本说明书并不对此进行限制），以使得共享平台可以据此确认机构1真实的身份信息；在步骤602中，

共享平台根据上述的成员加入申请，审核确认机构 1 的身份信息；在步骤 603 中，在对身份信息审核确认无误后，共享平台向机构 1 发送允许加入通知；在步骤 604 中，机构 1 向共享平台发送数字证书，该数字证书可由第三方 CA（Certificate Authority，证书颁发机构）发放或机构 1 自行产生，本说明书并不对此进行限制；在步骤 605 中，共享平台将数字证书与机构 1 的身份信息（即步骤 602 中审核确认的身份信息）相关联；在步骤 606 中，机构 1 针对预先生成的公私钥池（包含任意数量的公私钥对），用数字证书的私钥对公钥池数据进行签名，并将签名后的公钥池数据发送至共享平台；在步骤 607 中，共享平台通过数字证书的公钥对公钥池数据进行签名验证，在验证通过后将公钥池数据包含的公钥与机构 1 上述的身份信息相关联，从而将该公钥作为机构 1 的身份标识。

10 通过上述交互过程，可使机构 1 在共享平台处完成身份认证，从而将该机构 1 认证为共享平台相关联的成员，比如上述的成员 1。

[124] 步骤 501b，机构 2 通过在共享平台进行身份认证，加入为共享平台相关联的成员 2。

[125] 在一实施例中，机构 2 可以采用与机构 1 相类似的方式和处理过程，将自身认证为上述的成员 2；类似地，其他机构也可以据此将自身认证为相应的成员，此处不再赘述。

15

[126] 步骤 502a，成员 1 生成记录申请包，并上传至共享平台。

[127] 在一实施例中，成员 1 维护有一定的私有数据，而为了对这些私有数据进行共享，成员 1 可以为自身维护的私有数据生成对应的记录申请包，从而通过共享平台发布至索引区块链中。例如，图 7 是一示例性实施例提供的一种记录申请包的结构示意图。如图 7 所示，记录申请包可以包括主体标识 ID 的哈希值、主体描述信息、信息内容的哈希值、数据提供方的公钥、信息价格和数据提供方的私钥签名等，本说明书并不对此进行限制。

20

[128] 步骤 502b，成员 2 生成记录申请包，并上传至共享平台。

[129] 在一实施例中，成员 2 可以针对自身维护的私有数据生成如图 7 所示结构的记录申请包；类似地，其他成员可以分别针对自身维护的私有数据生成记录申请包，此处不再赘述。

25

[130] 步骤 503，共享平台验证收到的记录申请包，并针对通过验证的记录申请包，向索引区块链发布索引记录。

[131] 在一实施例中，共享平台可以提取记录申请包中包含的“数据提供方的公钥”，验证该公钥是否处于成员公钥池中，该成员公钥池内包含所有已认证的成员的公钥；如果处于成员公钥池中，表明该公钥属于有效的成员所有，则共享平台可以通过该公钥对记录申请包中包含的“数据提供方的私钥签名”进行验证，在验证通过后确定该记录申请包确实来自于对应成员，至此完成验证。若未通过验证，共享平台可以丢弃相应的记录申请包。

[132] 在一实施例中，共享平台针对已通过验证的记录申请包，可以生成相应的索引记录；其中，由于共享平台已经被配置为索引区块链的区块链节点，因而该共享平台可以通过向索引区块链中提交包含该索引记录的区块链交易，从而将该索引记录发布至索引区块链中，使得该索引记录被记载于索引区块链对应的区块链账本中。

[133] 以成员 1 上传的记录申请包为例：

[134] 在一实施例中，索引记录可以包含记录申请包中的“主体标识 ID 的哈希值”，该“主体标识 ID”是成员 1 所维护的私有数据的索引信息，比如当私有数据为商家销售记录时，主体标识 ID 可以包括“商家 ID+支付账号”，而通过生成相应的哈希值，使得索引信息“主体标识 ID”被处理为相应的密文索引，即上述的“主体标识 ID 的哈希值”。索引记录还可以包含成员 1 的服务地址，该服务地址用于指向该成员 1，以便于其他成员可以据此向成员 1 发起数据获取请求；其中，由于记录申请包由成员 1 发送至共享平台，因而共享平台在针对该记录申请包生成相应的索引记录时，可以自动将成员 1 的服务地址添加至该索引记录中。

[135] 在一实施例中，除了密文索引与服务地址之外，索引记录还可以包含记录申请包中的“主体信息描述”，该“主体信息描述”用于对成员 1 所维护的私有数据进行一定程度的描述，相当于成员 1 对于该私有数据的内容声明，以便于其他成员确定是否需要获得相关私有数据。譬如，对于上述的商家销售记录而言，该主体信息描述可以包括“2018 年 5 月~2018 年 6 月的记录”，表明其对应于这一时间段内的商家销售记录。

[136] 在一实施例中，除了密文索引与服务地址之外，索引记录还可以包含记录申请包中的“信息内容的哈希值”，该“信息内容”即成员 1 所维护的私有数据，通过生成该私有数据的哈希值，便于数据请求方在获得相关私有数据后，对数据内容的完整性和正确性予以检验，这将在步骤 509 进行描述。

[137] 在一实施例中，除了密文索引与服务地址之外，索引记录还可以包含信息价格，

该信息价格标示出了其他成员为获得相应的私有数据所需付出的代价，这一代价可以采用多种形式进行呈现，比如一定数额的资产凭证（如会员积分、代金券、货币余额等）、执行预设操作、提供指定的数据等，本说明书并不对此进行限制。

5 [138] 对于成员 2 或其他成员上传的记录申请包，共享平台均可以生成相应的索引记录并发布至索引区块链中，其生成过程和索引记录的内容均可以参考上述描述，此处不再赘述。

[139] 步骤 504，共享平台根据成员 1 发起的查询请求，查询索引区块链对应的区块链账本。

10 [140] 步骤 505，共享平台根据对区块链账本的查询情况，向成员 1 返回相应的查询结果。

[141] 在一实施例中，共享平台作为索引区块链的区块链节点，维护有索引区块链的区块链账本，该区块链账本包含索引区块链的全量数据，即记录有共享平台上传至索引区块链的所有索引记录。

15 [142] 在一实施例中，成员 1 至少可以获知其所需查询的私有数据的部分信息，比如对于上文所述的商家销售记录，成员 1 可以获知“商家 ID+支付账号”，即上述的主体标识 ID；相应地，成员 1 发起的查询请求中可以包括主体标识 ID 的哈希值，使得共享平台可以根据该哈希值对区块链账本进行检索，以获得相应的索引记录，并向成员 1 返回包含该索引记录的查询结果。

20 [143] 步骤 506，共享平台获取成员 1 发起的数据获取请求，并转发至相应的数据提供方。

[144] 在一实施例中，成员 1 根据查询结果中包含的索引记录，获取该索引记录中包含的服务地址，使得成员 1 可以向该服务地址发起数据获取请求。该服务地址由共享平台所维护，且共享平台能够明确该服务地址与相关成员之间的映射关系；比如，当该服务地址对应于成员 2 时，如果共享平台收到成员 1 向该服务地址发起的数据获取请求，
25 共享平台可以将该数据获取请求转发至成员 2，即成员 2 被作为相应的数据提供方。

[145] 步骤 507，成员 2 对收到的数据获取请求执行验证操作。

[146] 在一实施例中，图 8 是一示例性实施例提供的一种数据获取请求包的结构示意图。如图 8 所示，该数据获取请求包为上述数据获取请求的数据结构的表现形式，可以包括主体标识 ID 的哈希值、数据请求方的公钥、已有签名在索引区块链的位置、数据

请求方的私钥签名等,本说明书并不对此进行限制。针对如图8所示的数据获取请求包,成员2执行的验证操作可以包括:基于“已有签名在索引区块链的位置”确定相应的数据请求方是共享平台处的有效成员;提取“数据请求方的公钥”,对“数据请求方的私钥签名”进行验证。

5 [147] 步骤508,成员2生成响应包并返回至共享平台,由共享平台转发至成员1。

[148] 在一实施例中,成员2可以提取数据获取请求包含的“主体标识ID的哈希值”,并基于该密文索引对自身维护的私有数据进行检索,从而确定出相应的响应数据。当然,成员2维护的私有数据并不一定支持基于密文索引的检索操作;例如,成员2可以维护密文索引与明文索引的映射关系,据此确定出密文索引对应的明文索引,再基于明文索引对私有数据进行检索,从而确定出相应的响应数据。

10

[149] 在一实施例中,成员2对检索得到的响应数据进行封装,以生成相应的响应包。例如,图9是一示例性实施例提供的一种响应包的结构示意图。如图9所示,该响应包可以包括主体标识ID的哈希值、主体信息描述、信息内容的哈希值等,以便于成员1确定该响应包所对应的索引记录。响应包可以包括数据请求方的公钥,以使得共享平台据此确定响应包的发送目标为成员1,从而将该响应包发送至成员1。响应包可以包括加密后的数据内容,由成员2根据数据请求方的公钥对响应数据进行加密后得到。响应包可以包括数据提供方的私钥签名,即成员2的私钥签名。

15

[150] 步骤509,成员1针对收到的响应包执行验证操作。

[151] 在一实施例中,成员1对响应包的验证操作可以包括:根据数据提供方的公钥对私钥签名进行验证,若验证通过则表明该响应包确实来自于相应的数据提供方。通过成员1自身的公钥对加密后的数据内容进行解密处理,得到解密后数据,即成员2提供的上述响应数据;其中,由于成员1可能存在多个公钥,因而可以对响应包中包含的数据请求方的公钥进行验证,当确定该公钥为成员1自身拥有的公钥时,使用该公钥对加密后的数据内容进行解密。

20

[152] 在一实施例中,在获得解密后数据后,成员1可以生成该解密后数据的哈希值,并将其与响应包中的“信息内容的哈希值”进行比较;当比较结果一致时,可以确定响应包在传输过程中未受损。成员1可以将解密后数据的哈希值与先前获得的索引记录所包含的“信息内容的哈希值”进行比较;当比较结果一致时,可以确定成员2提供了正确数据,且响应包在传输过程中未被恶意替换。

25

[153] 在一实施例中，成员 1 可以确定解密后数据的描述内容；比如当解密后数据为商家销售记录时，描述内容可以包括该商家销售记录对应的月份，如果该月份为“2018 年 5 月-2018 年 6 月”，而主体信息描述为“2018 年 5 月~2018 年 6 月的记录”，表明成员 2 所提供的数据与其在索引区块链中声明的信息相符。

- 5 [154] 在一实施例中，对应于图 7 所示的“信息价格”，成员 1 需要向成员 2 付出相关代价后，才能够获得成员 2 提供的数据。以会员积分为例，共享平台可以作为各个成员之间的第三方，使得成员 1 可以根据索引记录中标注的信息价格，向共享平台转入相应数额的会员积分，使得共享平台将数据获取请求转发至成员 2；而当成员 2 返回响应包之后，或者在成员 1 确认收到响应包后，共享平台可以将相应的会员积分转至成员 2，
- 10 相当于成员 1 与成员 2 之间完成了一笔数据共享交易。相应地，当共享平台被配置为交易区块链的区块链节点时，共享平台可以向交易区块链提交一笔区块链交易，该区块链交易中包含成员 1 与成员 2 之间的上述数据共享交易的交易记录，以对该数据共享交易进行可靠记载，并且可以随时进行查询和核验。

[155] 步骤 510，成员 1 可以向共享平台发起投诉请求。

- 15 [156] 步骤 511，共享平台可以对投诉请求进行验证。

[157] 步骤 512，在投诉请求被确认为验证通过时，共享平台可以为索引区块链中对应的索引记录添加无效标识。

- [158] 在一实施例中，图 10 是一示例性实施例提供的一种投诉请求包的结构示意图。如图 10 所示，投诉请求包为上述投诉请求的数据结构的表现形式，可以包括：包类型，
- 20 用于表明当前数据包的类型为“投诉请求包”；被投诉数据的索引信息，比如被投诉数据对应的密文索引或索引记录；数据内容，明文数据内容；投诉原因，如获得的数据与索引记录中的“主体信息描述”不相符、获得的数据为虚假数据、获得的数据与自身或其他成员维护的数据雷同（比如成员 2 从成员 1 处购得数据后，生成并上传相应的记录申请包，以添加为自身维护的数据，侵犯成员 1 的权益）等，本说明书并不对此进行限制；
- 25 投诉者的私钥签名。

[159] 例如，当投诉原因为获得的数据与索引记录中的“主体信息描述”不相符时，共享平台可以根据“被投诉数据的索引信息”获取相关索引记录、提取出相关数据的哈希值，并对“数据内容”中的明文数据内容计算哈希值，若两个哈希值一致，表明该明文数据内容为相关索引记录对应的数据；进一步的，共享平台可以将该明文数据内容与

索引记录中声明的“主体信息描述”进行比较，从而确定两者是否存在不相符的情况。

[160] 在一实施例中，当投诉请求被确认为验证通过后，共享平台可以向索引区块链中提交一笔区块链交易，该区块链交易的内容包含：为被投诉数据的索引记录添加无效标识，使得该“被投诉数据的索引记录”在区块链账本中对应的状态参数发生变化，即被标记为无效状态。那么，在后续的数据共享过程中，被标记为无效状态的索引记录无法被共享，可由共享平台对此进行过滤与核验。

[161] 进一步的，共享平台还可以针对被投诉数据的数据提供方实施惩戒措施，比如限制其可获得数据的范围、提高其获取数据的价格、剥夺其成员身份等，本说明书并不对此进行限制。

10 [162] 在一实施例中，除了由成员进行投诉之外，共享平台可以对数据共享过程进行监督，以保障成员所提供数据的规范性和质量、打击恶意提供重复数据的成员等。例如，共享平台可以在成员的请求下，对可疑数据或其数据提供方进行核查；再例如，共享平台可以通过数据抽查的方式，以普通成员的身份从相关成员处获得相关数据，并对其数据的规范性、真实性、与声明的一致性等进行核实。

15 [163] 图 11 是一示例性实施例提供的一种设备的示意结构图。请参考图 11，在硬件层面，该设备包括处理器 1102、内部总线 1104、网络接口 1106、内存 1108 以及非易失性存储器 1110，当然还可能包括其他业务所需要的硬件。处理器 1102 从非易失性存储器 1110 中读取对应的计算机程序到内存 1108 中然后运行，在逻辑层面上形成数据共享装置。当然，除了软件实现方式之外，本说明书一个或多个实施例并不排除其他实现方式，
20 比如逻辑器件抑或软硬件结合的方式等等，也就是说以下处理流程的执行主体并不限定于各个逻辑单元，也可以是硬件或逻辑器件。

[164] 请参考图 12，在软件实施方式中，该数据共享装置应用于作为数据请求方的成员，所述装置可以包括：

25 [165] 确定单元 1201，确定索引区块链中记录的对应于目标数据的索引信息集合，所述索引信息集合包含所述目标数据的密文索引和所述目标数据的数据提供方的成员信息，所述索引信息集合由所述数据提供方共享至所述索引区块链；

[166] 请求单元 1202，通过共享平台向所述数据提供方发起数据获取请求，所述数据获取请求包含所述目标数据的密文索引；

[167] 接收单元 1203，接收所述共享平台返回的响应数据，所述响应数据由所述数据

请求方的身份公钥进行加密。

[168] 可选的, 所述共享平台被配置为所述索引区块链的节点; 所述确定单元 1201 具体用于:

[169] 根据已知的所述目标数据的特定信息, 生成相应的密文索引;

- 5 [170] 向所述共享平台发起查询请求, 所述查询请求中包含所述密文索引, 以指示所述共享平台从所述索引区块链中查询包含所述密文索引的索引信息集合; 或者, 下载所述共享平台维护的所述索引区块链的账本数据, 以查询出包含所述密文索引的索引信息集合。

- 10 [171] 可选的, 所述数据请求方被配置为所述索引区块链的节点; 所述确定单元 1201 具体用于:

[172] 根据已知的所述目标数据的特定信息, 生成相应的密文索引;

[173] 根据所述数据请求方维护的所述索引区块链的账本数据, 查询出包含所述密文索引的索引信息集合。

- 15 [174] 可选的, 所述数据获取请求还包含: 所述数据请求方的身份公钥、通过所述数据请求方的身份私钥生成的数据请求方签名, 以供所述数据提供方进行验证。

[175] 可选的, 所述响应数据中还包含: 通过所述数据提供方的身份私钥生成的数据提供方签名, 以供所述数据请求方进行验证。

[176] 可选的, 所述索引信息集合中包含所述目标数据的哈希值; 所述装置还包括:

[177] 计算单元 1204, 将所述响应数据对应的解密后数据进行哈希计算;

- 20 [178] 判断单元 1205, 当计算得到的哈希值与所述索引信息集合中的哈希值一致时, 确定所述解密后数据为所述目标数据。

[179] 可选的, 还包括:

[180] 投诉单元 1206, 向所述共享平台发起针对所述目标数据的投诉请求, 所述投诉请求中包含投诉理由和相关数据;

- 25 [181] 其中, 当所述投诉理由被所述共享平台或所述共享平台在所述索引区块链中调用的智能合约基于所述相关数据而验证为成立时, 所述索引信息集合在所述索引区块链中被添加无效标识。

[182] 可选的,还包括:

[183] 提交单元 1207,向所述索引区块链提交投诉类型的交易,以调取用于处理投诉的智能合约,其中所述交易包含投诉理由和相关数据;

[184] 其中,所述智能合约被用于根据所述相关数据验证所述投诉理由,并在所述投诉理由被验证为成立时,在所述索引区块链中为所述索引信息集合添加无效标识。

[185] 可选的,还包括:发布单元 1208 或发送单元 1209;

[186] 所述发布单元 1208 用于将所述数据请求方与所述数据提供方之间的数据共享事件发布至交易区块链,其中所述数据请求方被配置为所述交易区块链的节点;

[187] 所述发送单元 1209 用于将所述数据共享事件发送至所述共享平台,以由所述共享平台发布至所述交易区块链,其中所述共享平台被配置为所述交易区块链的节点。

[188] 图 13 是一示例性实施例提供的一种设备的示意结构图。请参考图 13,在硬件层面,该设备包括处理器 1302、内部总线 1304、网络接口 1306、内存 1308 以及非易失性存储器 1310,当然还可能包括其他业务所需要的硬件。处理器 1302 从非易失性存储器 1310 中读取对应的计算机程序到内存 1308 中然后运行,在逻辑层面上形成数据共享装置。当然,除了软件实现方式之外,本说明书一个或多个实施例并不排除其他实现方式,比如逻辑器件抑或软硬件结合的方式等等,也就是说以下处理流程的执行主体并不限定于各个逻辑单元,也可以是硬件或逻辑器件。

[189] 请参考图 14,在软件实施方式中,该数据共享装置应用于作为数据提供方的成员,所述装置可以包括:

[190] 共享单元 1401,将对应于目标数据的索引信息集合共享至索引区块链,所述索引信息集合包含所述目标数据的密文索引和所述数据提供方的成员信息;

[191] 接收单元 1402,接收数据请求方通过共享平台发起的数据获取请求,所述数据获取请求包含所述目标数据的密文索引;

[192] 返回单元 1403,通过所述共享平台向所述数据请求方返回响应数据,所述响应数据由所述数据请求方的身份公钥进行加密。

[193] 可选的,所述数据获取请求还包含:所述数据请求方的身份公钥、通过所述数据请求方的身份私钥生成的数据请求方签名,以供所述数据提供方进行验证。

[194] 可选的,所述响应数据中还包含:通过所述数据提供方的身份私钥生成的数据

提供方签名，以供所述数据请求方进行验证。

[195] 可选的，所述共享单元 1401 具体用于：

[196] 将所述索引信息集合发布至所述索引区块链，其中所述数据提供方被配置为所述索引区块链的节点；

5 [197] 或者，将所述索引信息集合提交至所述共享平台，以由所述共享平台发布至所述索引区块链，其中所述共享平台被配置为所述索引区块链的节点。

[198] 可选的，还包括：发布单元 1404 或发送单元 1405；

[199] 所述发布单元 1404 用于将所述数据请求方与所述数据提供方之间的数据共享事件发布至所述交易区块链，其中所述数据提供方被配置为交易区块链的节点；

10 [200] 所述发送单元 1405 用于将所述数据共享事件发送至所述共享平台，以由所述共享平台发布至所述交易区块链，其中所述共享平台被配置为所述交易区块链的节点。

[201] 图 15 是一示例性实施例提供的一种设备的示意结构图。请参考图 15，在硬件层面，该设备包括处理器 1502、内部总线 1504、网络接口 1506、内存 1508 以及非易失性存储器 1510，当然还可能包括其他业务所需要的硬件。处理器 1502 从非易失性存储器 1510 中读取对应的计算机程序到内存 1508 中然后运行，在逻辑层面上形成数据共享装置。当然，除了软件实现方式之外，本说明书一个或多个实施例并不排除其他实现方式，比如逻辑器件抑或软硬件结合的方式等等，也就是说以下处理流程的执行主体并不限定于各个逻辑单元，也可以是硬件或逻辑器件。

15 [202] 请参考图 16，在软件实施方式中，该数据共享装置应用于共享平台，所述装置可以包括：

[203] 第一发布单元 1601，将对应于目标数据的索引信息集合发布至索引区块链，所述索引信息集合包含所述目标数据的密文索引和所述目标数据的数据提供方的成员信息，所述索引信息集合由所述数据提供方提交至所述共享平台；

20 [204] 转发单元 1602，将数据请求方发起的数据获取请求转发至所述数据提供方，所述数据获取请求包含所述目标数据的密文索引；

[205] 返回单元 1603，将所述数据提供方提供的响应数据返回至所述数据请求方，所述响应数据由所述数据请求方的身份公钥进行加密。

[206] 可选的，还包括：

- [207] 第一接收单元 1604, 接收所述数据请求方发起的查询请求, 所述查询请求中包含根据已知的所述目标数据的特定信息生成的密文索引;
- [208] 查询单元 1605, 从所述索引区块链中查询包含所述密文索引的索引信息集合, 以告知所述数据请求方。
- 5 [209] 可选的, 还包括:
- [210] 第二接收单元 1606, 接收所述数据请求方向所述共享平台发起针对所述目标数据的投诉请求, 所述投诉请求中包含投诉理由和相关数据;
- [211] 添加单元 1607, 当基于所述相关数据验证所述投诉理由成立时, 在所述索引区块链中为所述索引信息集合添加无效标识。
- 10 [212] 可选的, 还包括:
- [213] 确定单元 1608, 确定所述数据请求方与所述数据提供方之间的数据共享事件;
- [214] 第二发布单元 1609, 将所述数据共享事件发布至所述交易区块链, 其中所述共享平台被配置为所述交易区块链的节点。
- [215] 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, 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。
- 15 [216] 在一个典型的配置中, 计算机包括一个或多个处理器 (CPU)、输入/输出接口、网络接口和内存。
- 20 [217] 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。
- [218] 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
- 25

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、磁盘存储、量子存储器、基于石墨烯的存储介质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。

- 5 [219] 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。
- 10 [220] 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。
- 15 [221] 在本说明书一个或多个实施例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一个或多个实施例。在本说明书一个或多个实施例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。
- 20 [222] 应当理解, 尽管在本说明书一个或多个实施例可能采用术语第一、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, 在不脱离本说明书一个或多个实施例范围的情况下, 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”。
- 25 [223] 以上所述仅为本说明书一个或多个实施例的较佳实施例而已, 并不用以限制本说明书一个或多个实施例, 凡在本说明书一个或多个实施例的精神和原则之内, 所做的任何修改、等同替换、改进等, 均应包含在本说明书一个或多个实施例保护的范围之内。

权利要求书

1. 一种数据共享系统, 包括:

成员, 每一成员分别维护有可共享的私有数据, 并为所述私有数据生成相应的密文索引信息, 所述密文索引信息包含对应的私有数据的密文索引和提供该私有数据的成员的信息;

共享平台, 所述共享平台分别连接至每一成员, 并将每一成员生成的密文索引信息记录于索引区块链, 以在所有成员之间进行共享; 所述共享平台将数据请求方成员发起的数据获取请求转发至数据提供方成员, 所述数据获取请求包含目标数据的密文索引, 且所述共享平台还将所述数据提供方成员返回的所述目标数据转发至所述数据请求方成员, 其中所述目标数据由所述数据请求方成员的身份公钥进行加密。

2. 根据权利要求 1 所述的系统, 所述共享平台被配置为所述索引区块链的区块链节点; 所述共享平台获取每一成员生成的密文索引信息, 并发布至所述索引区块链;

其中, 所述共享平台根据任一成员发起的信息查询请求, 在自身维护的索引区块链账本中查询对应的密文索引信息并返回至所述任一成员; 和/或, 至少一个成员下载所述共享平台维护的索引区块链账本, 以对密文索引信息进行查询。

3. 根据权利要求 1 所述的系统, 所述共享平台和每一成员分别被配置为所述索引区块链的区块链节点; 每一成员分别将生成的密文索引信息发布至所述索引区块链, 并通过自身维护的索引区块链账本对密文索引信息进行查询。

4. 根据权利要求 1 所述的系统, 所述共享平台被配置为交易区块链的区块链节点; 所述共享平台还将所述数据请求方成员与所述数据提供方成员之间的数据共享事件记录至所述交易区块链中。

5. 一种数据共享方法, 应用于作为数据请求方的成员, 所述方法包括:

确定索引区块链中记录的对应用于目标数据的索引信息集合, 所述索引信息集合包含所述目标数据的密文索引和所述目标数据的数据提供方的成员信息, 所述索引信息集合由所述数据提供方共享至所述索引区块链;

通过共享平台向所述数据提供方发起数据获取请求, 所述数据获取请求包含所述目标数据的密文索引;

接收所述共享平台返回的响应数据, 所述响应数据由所述数据请求方的身份公钥进行加密。

6. 根据权利要求 5 所述的方法, 所述共享平台被配置为所述索引区块链的节点; 所述确定索引区块链中记录的对应用于目标数据的索引信息集合, 包括:

根据已知的所述目标数据的特定信息,生成相应的密文索引;

向所述共享平台发起查询请求,所述查询请求中包含所述密文索引,以指示所述共享平台从所述索引区块链中查询包含所述密文索引的索引信息集合;或者,下载所述共享平台维护的所述索引区块链的账本数据,以查询出包含所述密文索引的索引信息集合。

- 5 7. 根据权利要求 5 所述的方法,所述数据请求方被配置为所述索引区块链的节点;所述确定索引区块链中记录的对应于目标数据的索引信息集合,包括:

根据已知的所述目标数据的特定信息,生成相应的密文索引;

根据所述数据请求方维护的所述索引区块链的账本数据,查询出包含所述密文索引的索引信息集合。

- 10 8. 根据权利要求 5 所述的方法,所述数据获取请求还包含:所述数据请求方的身份公钥、通过所述数据请求方的身份私钥生成的数据请求方签名,以供所述数据提供方进行验证。

9. 根据权利要求 5 所述的方法,所述响应数据中还包含:通过所述数据提供方的身份私钥生成的数据提供方签名,以供所述数据请求方进行验证。

- 15 10. 根据权利要求 5 所述的方法,所述索引信息集合中包含所述目标数据的哈希值;所述方法还包括:

将所述响应数据对应的解密后数据进行哈希计算;

当计算得到的哈希值与所述索引信息集合中的哈希值一致时,确定所述解密后数据为所述目标数据。

- 20 11. 根据权利要求 5 所述的方法,还包括:

向所述共享平台发起针对所述目标数据的投诉请求,所述投诉请求中包含投诉理由和相关数据;

其中,当所述投诉理由被所述共享平台或所述共享平台在所述索引区块链中调用的智能合约基于所述相关数据而验证为成立时,所述索引信息集合在所述索引区块链中被

- 25 添加无效标识。

12. 根据权利要求 5 所述的方法,还包括:

向所述索引区块链提交投诉类型的交易,以调取用于处理投诉的智能合约,其中所述交易包含投诉理由和相关数据;

- 30 其中,所述智能合约被用于根据所述相关数据验证所述投诉理由,并在所述投诉理由被验证为成立时,在所述索引区块链中为所述索引信息集合添加无效标识。

13. 根据权利要求 5 所述的方法,还包括:

将所述数据请求方与所述数据提供方之间的数据共享事件发布至交易区块链，其中所述数据请求方被配置为所述交易区块链的节点；

或者，将所述数据共享事件发送至所述共享平台，以由所述共享平台发布至所述交易区块链，其中所述共享平台被配置为所述交易区块链的节点。

- 5 14. 一种数据共享方法，应用于作为数据提供方的成员，所述方法包括：

将对应于目标数据的索引信息集合共享至索引区块链，所述索引信息集合包含所述目标数据的密文索引和所述数据提供方的成员信息；

接收数据请求方通过共享平台发起的数据获取请求，所述数据获取请求包含所述目标数据的密文索引；

- 10 通过所述共享平台向所述数据请求方返回响应数据，所述响应数据由所述数据请求方的身份公钥进行加密。

15 15. 根据权利要求 14 所述的方法，所述数据获取请求还包含：所述数据请求方的身份公钥、通过所述数据请求方的身份私钥生成的数据请求方签名，以供所述数据提供方进行验证。

- 15 16. 根据权利要求 14 所述的方法，所述响应数据中还包含：通过所述数据提供方的身份私钥生成的数据提供方签名，以供所述数据请求方进行验证。

17. 根据权利要求 14 所述的方法，所述将对应于目标数据的索引信息集合共享至索引区块链，包括：

- 20 将所述索引信息集合发布至所述索引区块链，其中所述数据提供方被配置为所述索引区块链的节点；

或者，将所述索引信息集合提交至所述共享平台，以由所述共享平台发布至所述索引区块链，其中所述共享平台被配置为所述索引区块链的节点。

18. 根据权利要求 14 所述的方法，还包括：

- 25 将所述数据请求方与所述数据提供方之间的数据共享事件发布至所述交易区块链，其中所述数据提供方被配置为交易区块链的节点；

或者，将所述数据共享事件发送至所述共享平台，以由所述共享平台发布至所述交易区块链，其中所述共享平台被配置为所述交易区块链的节点。

19. 一种数据共享方法，应用于共享平台，所述方法包括：

- 30 将对应于目标数据的索引信息集合发布至索引区块链，所述索引信息集合包含所述目标数据的密文索引和所述目标数据的数据提供方的成员信息，所述索引信息集合由所述数据提供方提交至所述共享平台；

将数据请求方发起的数据获取请求转发至所述数据提供方,所述数据获取请求包含所述目标数据的密文索引;

将所述数据提供方提供的响应数据返回至所述数据请求方,所述响应数据由所述数据请求方的身份公钥进行加密。

5 20. 根据权利要求 19 所述的方法,还包括:

接收所述数据请求方发起的查询请求,所述查询请求中包含根据已知的所述目标数据的特定信息生成的密文索引;

从所述索引区块链中查询包含所述密文索引的索引信息集合,以告知所述数据请求方。

10 21. 根据权利要求 19 所述的方法,还包括:

接收所述数据请求方向所述共享平台发起针对所述目标数据的投诉请求,所述投诉请求中包含投诉理由和相关数据;

当基于所述相关数据验证所述投诉理由成立时,在所述索引区块链中为所述索引信息集合添加无效标识。

15 22. 根据权利要求 19 所述的方法,还包括:

确定所述数据请求方与所述数据提供方之间的数据共享事件;

将所述数据共享事件发布至所述交易区块链,其中所述共享平台被配置为所述交易区块链的节点。

23. 一种数据共享装置,应用于作为数据请求方的成员,所述装置包括:

20 确定单元,确定索引区块链中记录的对应于目标数据的索引信息集合,所述索引信息集合包含所述目标数据的密文索引和所述目标数据的数据提供方的成员信息,所述索引信息集合由所述数据提供方共享至所述索引区块链;

请求单元,通过共享平台向所述数据提供方发起数据获取请求,所述数据获取请求包含所述目标数据的密文索引;

25 接收单元,接收所述共享平台返回的响应数据,所述响应数据由所述数据请求方的身份公钥进行加密。

24. 根据权利要求 23 所述的装置,所述共享平台被配置为所述索引区块链的节点;所述确定单元具体用于:

根据已知的所述目标数据的特定信息,生成相应的密文索引;

30 向所述共享平台发起查询请求,所述查询请求中包含所述密文索引,以指示所述共享平台从所述索引区块链中查询包含所述密文索引的索引信息集合;或者,下载所述共

享平台维护的所述索引区块链的账本数据，以查询出包含所述密文索引的索引信息集合。

25. 根据权利要求 23 所述的装置，所述数据请求方被配置为所述索引区块链的节点；所述确定单元具体用于：

根据已知的所述目标数据的特定信息，生成相应的密文索引；

5 根据所述数据请求方维护的所述索引区块链的账本数据，查询出包含所述密文索引的索引信息集合。

26. 根据权利要求 23 所述的装置，所述数据获取请求还包含：所述数据请求方的身份公钥、通过所述数据请求方的身份私钥生成的数据请求方签名，以供所述数据提供方进行验证。

10 27. 根据权利要求 23 所述的装置，所述响应数据中还包含：通过所述数据提供方的身份私钥生成的数据提供方签名，以供所述数据请求方进行验证。

28. 根据权利要求 23 所述的装置，所述索引信息集合中包含所述目标数据的哈希值；所述装置还包括：

计算单元，将所述响应数据对应的解密后数据进行哈希计算；

15 判断单元，当计算得到的哈希值与所述索引信息集合中的哈希值一致时，确定所述解密后数据为所述目标数据。

29. 根据权利要求 23 所述的装置，还包括：

投诉单元，向所述共享平台发起针对所述目标数据的投诉请求，所述投诉请求中包含投诉理由和相关数据；

20 其中，当所述投诉理由被所述共享平台或所述共享平台在所述索引区块链中调用的智能合约基于所述相关数据而验证为成立时，所述索引信息集合在所述索引区块链中被添加无效标识。

30. 根据权利要求 23 所述的装置，还包括：

25 提交单元，向所述索引区块链提交投诉类型的交易，以调取用于处理投诉的智能合约，其中所述交易包含投诉理由和相关数据；

其中，所述智能合约被用于根据所述相关数据验证所述投诉理由，并在所述投诉理由被验证为成立时，在所述索引区块链中为所述索引信息集合添加无效标识。

31. 根据权利要求 23 所述的装置，还包括：发布单元或发送单元；

30 所述发布单元用于将所述数据请求方与所述数据提供方之间的数据共享事件发布至交易区块链，其中所述数据请求方被配置为所述交易区块链的节点；

所述发送单元用于将所述数据共享事件发送至所述共享平台，以由所述共享平台发

布至所述交易区块链，其中所述共享平台被配置为所述交易区块链的节点。

32. 一种数据共享装置，应用于作为数据提供方的成员，所述装置包括：

共享单元，将对应于目标数据的索引信息集合共享至索引区块链，所述索引信息集合包含所述目标数据的密文索引和所述数据提供方的成员信息；

5 接收单元，接收数据请求方通过共享平台发起的数据获取请求，所述数据获取请求包含所述目标数据的密文索引；

返回单元，通过所述共享平台向所述数据请求方返回响应数据，所述响应数据由所述数据请求方的身份公钥进行加密。

33. 根据权利要求 32 所述的装置，所述数据获取请求还包含：所述数据请求方的身份公钥、通过所述数据请求方的身份私钥生成的数据请求方签名，以供所述数据提供方进行验证。

34. 根据权利要求 32 所述的装置，所述响应数据中还包含：通过所述数据提供方的身份私钥生成的数据提供方签名，以供所述数据请求方进行验证。

35. 根据权利要求 32 所述的装置，所述共享单元具体用于：

15 将所述索引信息集合发布至所述索引区块链，其中所述数据提供方被配置为所述索引区块链的节点；

或者，将所述索引信息集合提交至所述共享平台，以由所述共享平台发布至所述索引区块链，其中所述共享平台被配置为所述索引区块链的节点。

36. 根据权利要求 32 所述的装置，还包括：发布单元或发送单元；

20 所述发布单元用于将所述数据请求方与所述数据提供方之间的数据共享事件发布至所述交易区块链，其中所述数据提供方被配置为交易区块链的节点；

所述发送单元用于将所述数据共享事件发送至所述共享平台，以由所述共享平台发布至所述交易区块链，其中所述共享平台被配置为所述交易区块链的节点。

37. 一种数据共享装置，应用于共享平台，所述装置包括：

25 第一发布单元，将对应于目标数据的索引信息集合发布至索引区块链，所述索引信息集合包含所述目标数据的密文索引和所述目标数据的数据提供方的成员信息，所述索引信息集合由所述数据提供方提交至所述共享平台；

转发单元，将数据请求方发起的数据获取请求转发至所述数据提供方，所述数据获取请求包含所述目标数据的密文索引；

30 返回单元，将所述数据提供方提供的响应数据返回至所述数据请求方，所述响应数据由所述数据请求方的身份公钥进行加密。

38. 根据权利要求 37 所述的装置, 还包括:

第一接收单元, 接收所述数据请求方发起的查询请求, 所述查询请求中包含根据已知的所述目标数据的特定信息生成的密文索引;

5 查询单元, 从所述索引区块链中查询包含所述密文索引的索引信息集合, 以告知所述数据请求方。

39. 根据权利要求 37 所述的装置, 还包括:

第二接收单元, 接收所述数据请求方向所述共享平台发起针对所述目标数据的投诉请求, 所述投诉请求中包含投诉理由和相关数据;

10 添加单元, 当基于所述相关数据验证所述投诉理由成立时, 在所述索引区块链中为所述索引信息集合添加无效标识。

40. 根据权利要求 37 所述的装置, 还包括:

确定单元, 确定所述数据请求方与所述数据提供方之间的数据共享事件;

第二发布单元, 将所述数据共享事件发布至所述交易区块链, 其中所述共享平台被配置为所述交易区块链的节点。

15 41. 一种电子设备, 包括:

处理器;

用于存储处理器可执行指令的存储器;

其中, 所述处理器通过运行所述可执行指令以实现如权利要求 5-13 中任一项所述的方法。

20 42. 一种电子设备, 包括:

处理器;

用于存储处理器可执行指令的存储器;

其中, 所述处理器通过运行所述可执行指令以实现如权利要求 14-18 中任一项所述的方法。

25 43. 一种电子设备, 包括:

处理器;

用于存储处理器可执行指令的存储器;

其中, 所述处理器通过运行所述可执行指令以实现如权利要求 19-22 中任一项所述的方法。