

一种区块链数据授权访问方法及装置、设备

相关申请的交叉引用

本申请要求在2020年04月22日提交中国专利局、申请号为202010322631.0、
申请名称为“一种区块链数据授权访问方法及装置”的中国专利申请的优先
5 权，其全部内容通过引用结合在本申请中。

技术领域

本发明涉及区块链技术领域，尤其涉及一种区块链数据授权访问方法及
装置、设备。

10

背景技术

在办理一些银行业务时，为了避免用户重复填写开卡信息，卡服务商可
以利用区块链直接提供数据服务给开卡行。但为了保护数据的所有权和隐私，
卡服务商不能直接获取用户信息明文，并且开卡方获得数据需要经过用户授
15 权。因此，需要设计一种授权方案，在保证数据服务的同时，保护数据隐私。

发明内容

本发明实施例提供一种区块链数据授权访问方法及装置、设备，用以实
现受用户控制的数据访问授权，保护数据隐私。

20 第一方面，本发明实施例提供一种区块链数据授权访问方法，包括：

区块链平台获取第三方机构的数据访问请求，所述数据访问请求包括访
问数据的用户标识、数据范围和签名的随机数；所述签名的随机数是所述第
三方机构接收到用户端发送的随机数后签名生成的；所述用户端发送的随机
数是所述用户端接收到所述第三方机构发送的授权请求并在确定对所述第三
25 方机构进行数据授权后生成的；

所述区块链平台对所述签名的随机数和所述数据范围进行验证；

所述区块链平台在确认验证通过后，将所述用户标识对应的数据密文发送给所述第三方机构，以使所述第三方机构使用所述用户端发送的数据私钥对所述数据密文进行解密。

上述技术方案中，区块链平台通过依据用户端授权后的数据验证信息对
5 第三方机构的数据访问请求中的随机数、数据范围等信息进行验证，使得用
户的数据可以精确控制，用户同时可以控制第三方访问数据的范围和时效。
由于第三方机构每次发送授权请求后，用户端都会产生一个随机数，从而可
以实现每次授权请求的随机数不同，从而可以保证一次授权只能访问一次，
如果第三方机构需要再次访问，则需要再次向用户端发送授权请求，从而可
10 以用户对自己的隐私数据的可控，提高数据保护力度。

可选的，所述区块链平台对所述签名的随机数、所述数据范围和所述数
据访问请求的计时器进行验证，包括：

所述区块链平台使用第三公钥对所述签名的随机数进行验证，使用所述
用户端发送的数据访问的数据范围对所述数据范围进行验证。

15 可选的，所述区块链平台在将所述用户标识对应的数据密文发送给所述
第三方机构之前，还包括：

所述区块链平台确认所述数据访问请求的计时器未超时，所述数据访问
请求的计时器是在接收到所述用户端发送的数据验证信息后启动的。

20 可选的，所述区块链平台在获取第三方机构的数据访问请求之前，还包
括：

所述区块链平台获取用户端发送的数据验证信息，所述数据验证信息包
括随机数、第三方公钥、数据访问的数据范围和时间；

所述区块链平台根据所述数据访问的时间启动数据访问请求的计时器，
并将所述随机数、所述第三方公钥和所述数据访问的数据范围进行登记。

25 可选的，所述区块链平台在获取用户端发送的数据验证信息之前，还包
括：

所述区块链平台获取所述用户端发送的数据存储信息；所述数据存储信

息包括用户标识和所述用户标识对应的数据密文；所述数据密文是所述用户端使用所述用户端的对称秘钥对数据进行加密后得到的；

所述区块链平台将所述用户标记和所述用户标识对应的数据密文进行存储。

- 5 可选的，所述区块链平台将所述用户标记和所述用户标识对应的数据密文进行存储之后，还包括：

所述区块链平台获取所述用户端发送的新数据密文，所述新数据密文是所述用户端使用对称秘钥对新数据进行加密后得到的；

所述区块链平台将所述新数据密文覆盖所述数据密文。

- 10 可选的，所述区块链平台将所述用户标记和所述用户标识对应的数据密文进行存储之后，还包括：

所述区块链平台获取所述用户端发送的数据请求；

所述区块链平台向所述用户端发送所述数据密文，以使所述用户端对所述数据密文解密后使用新的对称秘钥对所述数据进行加密；

- 15 所述区块链平台获取所述用户端发送的数据存储请求，所述数据存储请求包括所述用户端使用新的对称秘钥加密所述数据的新数据密文；

所述区块链平台将所述新数据密文覆盖所述数据密文。

第二方面，本发明实施例提供一种区块链数据授权访问装置，包括：

- 20 获取单元，用于获取第三方机构的数据访问请求，所述数据访问请求包括访问数据的用户标识、数据范围和签名的随机数；所述签名的随机数是所述第三方机构接收到用户端发送的随机数后签名生成的；所述用户端发送的随机数是所述用户端接收到所述第三方机构发送的授权请求并在确定对所述第三方机构进行数据授权后生成的；

处理单元，用于对所述签名的随机数和所述数据范围；

- 25 发送单元，用于在确认验证通过后，将所述用户标识对应的数据密文发送给所述第三方机构，以使所述第三方机构使用所述用户端发送的数据私钥对所述数据密文进行解密。

可选的，所述处理单元具体用于：

使用第三公钥对所述签名的随机数进行验证，使用所述用户端发送的数据访问的数据范围对所述数据范围进行验证。

可选的，所述处理单元还用于：

- 5 在将所述用户标识对应的数据密文发送给所述第三方机构之前，确认所述数据访问请求的计时器未超时，所述数据访问请求的计时器是在接收到所述用户端发送的数据验证信息后启动的。

可选的，所述处理单元还用于：

- 10 在获取第三方机构的数据访问请求之前，获取用户端发送的数据验证信息，所述数据验证信息包括随机数、第三方公钥、数据访问的数据范围和时
间；

根据所述数据访问的时间启动数据访问请求的计时器，并将所述随机数、所述第三方公钥和所述数据访问的数据范围进行登记。

可选的，所述处理单元还用于：

- 15 在获取用户端发送的数据验证信息之前，获取所述用户端发送的数据存储信息；所述数据存储信息包括用户标识和所述用户标识对应的数据密文；所述数据密文是所述用户端使用所述用户端的对称密钥对数据进行加密后得到的；

将所述用户标记和所述用户标识对应的数据密文进行存储。

- 20 可选的，所述处理单元还用于：

将所述用户标记和所述用户标识对应的数据密文进行存储之后，获取所述用户端发送的新数据密文，所述新数据密文是所述用户端使用对称密钥对新数据进行加密后得到的；

将所述新数据密文覆盖所述数据密文。

- 25 可选的，所述处理单元还用于：

将所述用户标记和所述用户标识对应的数据密文进行存储之后，获取所述用户端发送的数据请求；

向所述用户端发送所述数据密文，以使所述用户端对所述数据密文解密后使用新的对称密钥对所述数据进行加密；

获取所述用户端发送的数据存储请求，所述数据存储请求包括所述用户端使用新的对称密钥加密所述数据的新数据密文；

5 将所述新数据密文覆盖所述数据密文。

第三方面，本发明实施例还提供一种计算设备，包括：

存储器，用于存储程序指令；

处理器，用于调用所述存储器中存储的程序指令，按照获得的程序执行上述区块链数据授权访问方法。

10 第四方面，本发明实施例还提供一种计算机可读非易失性存储介质，包括计算机可读指令，当计算机读取并执行所述计算机可读指令时，使得计算机执行上述区块链数据授权访问方法。

第五方面，本发明实施例提供了一种区块链数据授权访问设备，其特征在于，包括：

15 至少一个处理器；以及，

与所述至少一个处理器通信连接的存储器；其中，

所述存储器存储有可被所述至少一个处理器执行的指令，所述指令被所述至少一个处理器执行，以使所述至少一个处理器能够执行上述第一方面所述的方法。

20

附图说明

为了更清楚地说明本发明实施例中的技术方案，下面将对实施例描述中所需要使用的附图作简要介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域的普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

25

图 1 为本发明实施例提供的一种系统架构的示意图；

图 2 为本发明实施例提供的一种区块链数据授权访问方法的流程示意图；

图 3 为本发明实施例提供的一种数据存储的示意图;

图 4 为本发明实施例提供的一种数据访问的示意图;

图 5 为本发明实施例提供的一种数据变更的示意图;

图 6 为本发明实施例提供的一种密钥变更的示意图;

5 图 7 为本发明实施例提供的一种区块链数据授权访问装置的结构示意图;

图 8 为本发明实施例提供的一种区块链数据授权访问设备的结构示意图。

具体实施方式

为了使本发明的目的、技术方案和优点更加清楚，下面将结合附图对本发明作进一步地详细描述，显然，所描述的实施例仅仅是本发明一部分实施例，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它实施例，都属于本发明保护的范围。

图 1 示例性的示出了本发明实施例所适用的一种系统架构，该系统架构可以包括多个用户端 100、区块链平台 200 和多个第三方机构 300。

其中，用户端 100 用于与区块链平台 200 进行通信，将数据密文发送给区块链平台 200 进行上链存储。

第三方机构 300 用于在用户端 100 授权的情况下从区块链平台 200 访问用户端 100 存储的数据密文。

20 区块链平台 200 由多个区块链节点 210，与用户端 100 和第三方机构 300 进行通信，用于处理和存储用户端 100 发送的数据密文，并在对第三方机构 300 发送的数据访问请求验证通过后向第三方机构 300 发送用户端 100 存储的数据密文。该多个区块链节点 210 可以相互连接通信，每个区块链节点 210 中包括多个区块，区块用于存储用户端 100 发送的数据密文。

25 需要说明的是，上述图 1 所示的结构仅是一种示例，本发明实施例对此不做限定。

基于上述描述，图 2 详细的示出了本发明实施例提供的一种区块链数据

授权访问方法的流程，该流程可以由区块链数据授权访问装置执行，该装置可以位于区块链节点中，也可以是该区块链节点。

如图 2 所示，该流程具体包括：

步骤 201，区块链平台获取第三方机构的数据访问请求。

- 5 该数据访问请求中可以包括访问数据的用户标识、数据范围和签名的随机数，其中，签名的随机数是第三方机构接收到用户端发送的随机数后签名生成的。用户端发送的随机数是用户端接收到第三方机构发送的授权请求并在确定对第三方机构进行数据授权后生成的。

10 区块链平台在获取第三方机构的数据访问请求之前，获取用户端发送的数据验证信息，该数据验证信息可以包括随机数、第三方公钥、数据访问的数据范围和时间。然后根据数据访问的时间启动数据访问请求的计时器，并将随机数、第三方公钥和数据访问的数据范围进行登记。该第三方公钥是第三方机构的公钥。

15 同时，区块链平台还可以获取用户端发送的数据存储信息，该数据存储信息包括用户标识和用户标识对应的数据密文。其中，数据密文是用户端使用用户端的对称密钥对数据进行加密后得到的。区块链平台将用户标识和用户标识对应的数据密文进行存储。

举例来说，如图 3 所示，用户端将数据存储至区块链数据平台的步骤如下：

- 20 (1)、用户端生成对称密钥；
- (2)、用户端使用自身的对称密钥对数据进行加密，并将加密后的数据发送到区块链数据平台；
- (3)、区块链数据平台存储加密后的数据。

25 当第三方机构进行数据授权访问时，如图 4 所示，第三方机构向用户授权数据访问的步骤如下：

- (1)、第三方机构向用户端发送授权请求，包括数据的范围、以及本机构的公钥。

(2)、用户端确定授权后，生成一个随机的 nonce（随机数）；

(3)、用户端将生成的 nonce、第三方公钥、数据访问的范围和时限发送给区块链平台；同时将相同的 nonce 及数据的对称秘钥发送给第三方机构。

(4)、区块链平台收到请求后将 nonce、第三方公钥和数据访问范围进行登记，然后根据数据请求时限设定一个计时器。

步骤 202，所述区块链平台对所述签名的随机数和所述数据范围进行验证。

具体的，区块链平台可以使用第三公钥对签名的随机数进行验证，通过第三公钥可以验证签名是否正确。使用用户端发送的数据访问的数据范围对数据范围进行验证，数据范围相同表示验证通过。

由于第三方机构每次发送授权请求后，用户端都会产生一个随机数，从而可以实现每次授权请求的随机数不同，从而可以保证一次授权只能访问一次，如果第三方机构需要再次访问，则需要再次向用户端发送授权请求，从而可以用用户对自己的隐私数据的可控，提高数据保护力度。

此外还可以对第三方机构的数据访问请求的时间进行验证，用来验证第三方机构本次数据访问是否超时，若已超时，也表示验证不通过。主要是确认数据访问请求的计时器是否超时。其中，数据访问请求的计时器是在接收到用户端发送的数据验证信息后启动的。

通过设置计时器的方式来限定第三方机构的数据访问的时间，可以进一步的实现一次访问一次授权的功能。

也就是说，如图 4 所示，区块链平台通过部署的智能合约对 nonce 签名进行验证，对请求的数据范围进行验证，同时判断计时器是否超时。

步骤 203，所述区块链平台在确认验证通过后，将所述用户标识对应的数据密文发送给所述第三方机构。

在步骤 202 中区块链平台确认验证通过后，就可以将相应的数据密文发送给第三方机构。如图 4 所示，如果条件都满足，则将相应的数据密文返回给第三方机构；否则拒绝第三方机构的请求。同时通知用户端。也就是说，条件都满足之后，区块链平台依据数据范围，将符合数据范围的相应的数据

密文发送给第三方机构。

第三方机构收到数据密文后，使用用户端发送的数据密钥对数据进行解密，获得数据明文。

需要说明的是，用户端在将数据存储到区块链平台之后，还可以对数据进行变更和密钥变更，具体的：

数据变更可以为：

区块链平台获取用户端发送的新数据密文，新数据密文是用户端使用对称密钥对新数据进行加密后得到的。区块链平台将新数据密文覆盖数据密文。

区块链平台获取所述用户端发送的数据请求；

10 密钥变更可以为：

首先，区块链平台向所述用户端发送数据密文，以使用户端对数据密文解密后使用新的对称密钥对数据进行加密。然后区块链平台获取用户端发送的数据存储请求，数据存储请求包括用户端使用新的对称密钥加密数据的新数据密文。最后区块链平台将新数据密文覆盖数据密文。

15 举例来说，如图 5 所示，数据变更的步骤如下：

- (1)、用户端用密钥对新数据进行加密；
- (2)、用户端将加密后的数据发送到区块链平台；
- (3)、区块链平台用新数据密文覆盖旧数据密文。

如图 6 所示，用户的数据密钥可以定期进行变更，或手动进行变更，密钥变更的步骤如下：

- (1)、用户端向区块链平台请求数据；
- (2)、区块链平台返回数据；
- (3)、用户端用旧密钥对数据进行解密，并用新密钥对数据进行加密；
- (4)、用户端将加密后的新数据发送给区块链平台；
- 25 (5)、区块链平台覆盖旧数据。

为了更好的解释本发明实施例，下面将在具体实施场景下来描述上述数据授权访问的过程。

实施例一：一键通业务的用户授权。

用户在用户端使用数据和私钥管理 APP 的一些功能，功能包括：私钥生成、数据加密和解密、随机 nonce 生成等功能；

5 第三方机构为银行发卡平台，可以生成一对公私钥，功能包括签名、数据解密；

区块链平台采用 Hyperledger fabric 平台，通过链码实现用户数据存储、签名验证、数据范围过滤、计时器等功能，对外提供 RESTful API 接口。

三方可以通过互联网连接，通过 http 协议进行相互访问。

其中，数据存储和数据授权流程：

10 (1)、用户端的 APP 使用 AES 对称加密算法生成对称密钥，并对个人信息进行加密，得到数据密文，调用区块链平台上的智能合约的数据存储接口将数据密文存储到区块链平台中。

(2)、第三方机构组建授权请求，请求包括用户姓名、手机号、身份证号等信息范围，以及生成公钥。

15 (3)、用户端的 APP 收到第三方机构的授权请求，通知用户进行授权。用户确认范围，如果同意授权并选择授权的时限后，用户端的 APP 生成一个随机的 nonce 串；否则，向第三方机构返回拒绝信息，流程结束。

(4)、用户端的 APP 通过调用区块链平台的智能合约的授权接口，将 nonce 串、第三机构的公钥、数据范围、时限发送给区块链平台；同时用户端的 APP 20 将 nonce 串和 AES 密钥发送给第三方机构(网络数据可用 tls/ssl 加密)；

(5)、区块链平台的智能合约的授权接口收到用户端的 APP 的信息后，登记 nonce 串、第三方机构的公钥、数据范围，并根据时限设置一个计时器；

(6)、第三方机构收到用户端的 APP 发送的信息后，对 nonce 串用自己的私钥进行签名，并组建数据请求，包括数据访问范围、签名等信息，并发送 25 给区块链平台的智能合约的数据访问接口。

(7)、区块链平台的智能合约的数据访问接口收到请求后，首先用登记的 nonce 和第三方机构的私钥对签名进行验证，然后判断数据访问范围是否匹配，

以及计时器是否超时。如果条件都满足，则从用户信息中过滤出特定数据范围内的数据密文，返回给第三方机构，同时通知给用户端的 APP 该第三方机构访问数据的通知；否则，拒绝第三方机构的请求。

5 (8)、第三方机构收到区块链返回的数据后，用第(6)步中收到的数据密钥对数据密文进行解密，获得用户数据明文。

需要说的是，在实际应用的过程中，上述区块链平台采用其他框架；或者采用非区块链的数据平台。上述用户端 APP 替换成公众号服务、网页服务、电脑客户端等形式。上述用户端密钥可以保存在 TEE 等可信执行环境。上述加解密功能可以在 TEE 或加密机中进行。上述加解密算法可以采用 DES、
10 3DES、国密等算法。可以设置更多的访问条件，如数据访问次数、登记到数据本身的限制条件。上述用户可以是一个机构，数据可以机构数据，实现机构间的数据授权访问。

上述实施例表明，区块链平台获取第三方机构的数据访问请求，数据访问请求包括访问数据的用户标识、数据范围和签名的随机数，签名的随机数是所述第三方机构接收到用户端发送的随机数后签名生成的，用户端发送的随机数是用户端接收到第三方机构发送的授权请求并在确定对第三方机构进行数据授权后生成的，对签名的随机数和数据范围进行验证，在验证通过后，将用户标识对应的数据密文发送给第三方机构，以使第三方机构使用用户端发送的数据私钥对数据密文进行解密。区块链平台通过依据用户端授权后的
20 数据验证信息对第三方机构的数据访问请求中的随机数、数据范围、数据访问的时间等信息进行验证，使得用户的数据可以精确控制，用户同时可以控制第三方访问数据的范围和时效。由于第三方机构每次发送授权请求后，用户端都会产生一个随机数，从而可以实现每次授权请求的随机数不同，从而可以保证一次授权只能访问一次，如果第三方机构需要再次访问，则需要再次向用户端发送授权请求，从而可以用户对自己的隐私数据的可控，提高数据保护力度。
25

基于相同的技术构思，图 7 示例性的示出了本发明实施例提供的一种区

区块链数据授权访问装置的结构，该装置可以执行区块链数据授权访问流程。

如图 7 所示，该装置具体包括：

获取单元 701，用于获取第三方机构的数据访问请求，所述数据访问请求包括访问数据的用户标识、数据范围和签名的随机数；所述签名的随机数是
5 所述第三方机构接收到用户端发送的随机数后签名生成的；所述用户端发送的随机数是所述用户端接收到所述第三方机构发送的授权请求并在确定对所述第三方机构进行数据授权后生成的；

处理单元 702，用于对所述签名的随机数和所述数据范围；

发送单元 703，用于在确认验证通过后，将所述用户标识对应的数据密文
10 发送给所述第三方机构，以使所述第三方机构使用所述用户端发送的数据私钥对所述数据密文进行解密。

可选的，所述处理单元 702 具体用于：

使用第三公钥对所述签名的随机数进行验证，使用所述用户端发送的数据访问的数据范围对所述数据范围进行验证。

15 可选的，所述处理单元 702 还用于：

在将所述用户标识对应的数据密文发送给所述第三方机构之前，确认所述数据访问请求的计时器未超时，所述数据访问请求的计时器是在接收到所述用户端发送的数据验证信息后启动的。

可选的，所述处理单元 702 还用于：

20 在获取第三方机构的数据访问请求之前，获取用户端发送的数据验证信息，所述数据验证信息包括随机数、第三方公钥、数据访问的数据范围和时
间；

根据所述数据访问的时间启动数据访问请求的计时器，并将所述随机数、所述第三方公钥和所述数据访问的数据范围进行登记。

25 可选的，所述处理单元 702 还用于：

在获取用户端发送的数据验证信息之前，获取所述用户端发送的数据存储信息；所述数据存储信息包括用户标识和所述用户标识对应的数据密文；

所述数据密文是所述用户端使用所述用户端的对称密钥对数据进行加密后得到的;

将所述用户标记和所述用户标识对应的数据密文进行存储。

可选的,所述处理单元 702 还用于:

- 5 将所述用户标记和所述用户标识对应的数据密文进行存储之后,获取所述用户端发送的新数据密文,所述新数据密文是所述用户端使用对称密钥对新数据进行加密后得到的;

将所述新数据密文覆盖所述数据密文。

可选的,所述处理单元 702 还用于:

- 10 将所述用户标记和所述用户标识对应的数据密文进行存储之后,获取所述用户端发送的数据请求;

向所述用户端发送所述数据密文,以使所述用户端对所述数据密文解密后使用新的对称密钥对所述数据进行加密;

- 15 获取所述用户端发送的数据存储请求,所述数据存储请求包括所述用户端使用新的对称密钥加密所述数据的新数据密文;

将所述新数据密文覆盖所述数据密文。

- 20 基于相同的技术构思,本发明实施例提供一种区块链数据授权访问设备。至少一个处理器;以及,与所述至少一个处理器通信连接的存储器;所述存储器存储有可被所述至少一个处理器执行的指令,所述指令被所述至少一个处理器执行,以使所述至少一个处理器能够执行上述实施例中的区块链数据授权访问方法。

以一个处理器为例,图 8 为本发明实施例提供的区块链数据授权访问设备的结构,该区块链数据授权访问设备 800 包括:收发器 801、处理器 802、存储器 803 和总线系统 804;

- 25 其中,存储器 803,用于存放程序。具体地,程序可以包括程序代码,程序代码包括计算机操作指令。存储器 803 可能为随机存取存储器(random access memory,简称 RAM),也可能为非易失性存储器(non-volatile memory),

例如至少一个磁盘存储器。图中仅示出了一个存储器，当然，存储器也可以根据需要，设置为多个。存储器 803 也可以是处理器 802 中的存储器。

存储器 803 存储了如下的元素，可执行模块或者数据结构，或者它们的子集，或者它们的扩展集：

5 操作指令：包括各种操作指令，用于实现各种操作。

操作系统：包括各种系统程序，用于实现各种基础业务以及处理基于硬件的任务。

上述本发明实施例区块链数据授权访问方法可以应用于处理器 802 中，或者说由处理器 802 实现。处理器 802 可能是一种集成电路芯片，具有信号
10 的处理能力。在实现过程中，上述区块链数据授权访问方法的各步骤可以通过处理器 802 中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器 802 可以是通用处理器、数字信号处理器(DSP)、专用集成电路(ASIC)、现场可编程门阵列(FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。可以实现或者执行本申请实施例中的公开的各方法、
15 步骤及逻辑框图。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。结合本发明实施例所公开的方法的步骤可以直接体现为硬件译码处理器执行完成，或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于
20 存储器 803，处理器 802 读取存储器 803 中的信息，结合其硬件执行以下步骤：

收发器 801，用于获取第三方机构的数据访问请求，所述数据访问请求包括访问数据的用户标识、数据范围和签名的随机数；所述签名的随机数是所述第三方机构接收到用户端发送的随机数后签名生成的；所述用户端发送的
25 随机数是所述用户端接收到所述第三方机构发送的授权请求并在确定对所述第三方机构进行数据授权后生成的；

处理器 802，用于对所述签名的随机数和所述数据范围；

收发器 801, 用于在确认验证通过后, 将所述用户标识对应的数据密文发送给所述第三方机构, 以使所述第三方机构使用所述用户端发送的数据私钥对所述数据密文进行解密。

可选的, 所述处理器 802 具体用于:

- 5 使用第三公钥对所述签名的随机数进行验证, 使用所述用户端发送的数据访问的数据范围对所述数据范围进行验证。

可选的, 所述处理器 802 还用于:

- 10 在将所述用户标识对应的数据密文发送给所述第三方机构之前, 确认所述数据访问请求的计时器未超时, 所述数据访问请求的计时器是在接收到所述用户端发送的数据验证信息后启动的。

可选的, 所述处理器 802 还用于:

- 15 在获取第三方机构的数据访问请求之前, 获取用户端发送的数据验证信息, 所述数据验证信息包括随机数、第三方公钥、数据访问的数据范围和时
间;
15 根据所述数据访问的时间启动数据访问请求的计时器, 并将所述随机数、所述第三方公钥和所述数据访问的数据范围进行登记。

可选的, 所述处理器 802 还用于:

- 20 在获取用户端发送的数据验证信息之前, 获取所述用户端发送的数据存储信息; 所述数据存储信息包括用户标识和所述用户标识对应的数据密文;
20 所述数据密文是所述用户端使用所述用户端的对称秘钥对数据进行加密后得到的;

将所述用户标记和所述用户标识对应的数据密文进行存储。

可选的, 所述处理器 802 还用于:

- 25 将所述用户标记和所述用户标识对应的数据密文进行存储之后, 获取所述用户端发送的新数据密文, 所述新数据密文是所述用户端使用对称秘钥对新数据进行加密后得到的;

将所述新数据密文覆盖所述数据密文。

可选的, 所述处理器 802 还用于:

将所述用户标记和所述用户标识对应的数据密文进行存储之后, 获取所述用户端发送的数据请求;

向所述用户端发送所述数据密文, 以使所述用户端对所述数据密文解密后使用新的对称密钥对所述数据进行加密;

获取所述用户端发送的数据存储请求, 所述数据存储请求包括所述用户端使用新的对称密钥加密所述数据的新数据密文;

将所述新数据密文覆盖所述数据密文。

本领域技术人员可以理解实现上述实施例方法中的全部或部分步骤是可以通过程序来指令相关的硬件来完成, 该程序存储在一个存储介质中, 包括若干指令用以使得一个设备 (可以是单片机, 芯片等) 或处理器 (processor) 执行本申请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、移动硬盘、只读存储器 (ROM, Read-Only Memory)、随机存取存储器 (RAM, Random Access Memory)、磁碟或者光盘等各种可以存储程序代码的介质。

基于相同的技术构思, 本发明实施例还提供了一种计算设备, 包括:

存储器, 用于存储程序指令;

处理器, 用于调用存储器中存储的程序指令, 按照获得的程序执行上述区块链数据授权访问方法。

基于相同的技术构思, 本发明实施例还提供了一种计算机可读非易失性存储介质, 包括计算机可读指令, 当计算机读取并执行计算机可读指令时, 使得计算机执行上述区块链数据授权访问方法。

本发明是参照根据本发明实施例的方法、设备 (系统)、和计算机程序产品的流程图和 / 或方框图来描述的。应理解可由计算机程序指令实现流程图和 / 或方框图中的每一流程和 / 或方框、以及流程图和 / 或方框图中的流程和 / 或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器, 使得通

过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能的装置。

5 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能。

10 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能的步骤。

尽管已描述了本发明的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例作出另外的变更和修改。所以，所附权利要求要求意欲解释为包括优选实施例以及落入本发明范围的所有变更和修改。

15 显然，本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样，倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。