

权利要求

1、一种区块链数据授权访问方法，其特征在于，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
5 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；

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
10 对所述数据密文进行解密。

2、如权利要求 1 所述的方法，其特征在于，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，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
15 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。

3、如权利要求 1 所述的方法，其特征在于，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 4、如权利要求 1 至 3 任一项所述的方法，其特征在于，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，
25 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。

5、如权利要求 4 所述的方法，其特征在于，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；

5 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。

6、如权利要求5所述的方法，其特征在于，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
10 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。

7、如权利要求5所述的方法，其特征在于，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；

15 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；

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。

20 8、一种区块链数据授权访问装置，其特征在于，包括：

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
25 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进行验证；

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。

9、如权利要求 8 所述的装置，其特征在于，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。

10、如权利要求 8 所述的装置，其特征在于，所述处理单元还用于：

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。

11、如权利要求 8 至 10 任一项所述的装置，其特征在于，所述处理单元还用于：

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。

12、如权利要求 11 所述的装置，其特征在于，所述处理单元还用于：

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。

13、如权利要求 12 所述的装置，其特征在于，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。

14、如权利要求 12 所述的装置，其特征在于，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；

5 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。

15、一种计算设备，其特征在于，包括：

10 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权利要求 1 至 7 任一项所述的方法。

16、一种计算机可读非易失性存储介质，其特征在于，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，使得计算机执行如权利要求 1 至 7 任一项所述的方法。

17、一种区块链数据授权访问设备，其特征在于，包括：

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，

20 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权利要求 1 至 7 任一权利要求所述的方法。