

权利要求书

1、一种存储区块链账户私钥的方法，包括：

安装于用户的用户设备上的私钥管理程序获取私钥集合；所述私钥集合包括所述用户注册的区块链账户的至少一个账户私钥；

获取所述用户提供的加密密钥；

使用所述加密密钥对所述私钥集合进行加密，并存储加密后的所述私钥集合。

2、如权利要求 1 所述的方法，所述私钥集合还包括至少一个其他用户提供给所述用户的账户私钥；针对每个其他用户，该其他用户提供给所述用户的账户私钥是该其他用户注册的区块链账户的账户私钥。

3、如权利要求 1 所述的方法，所述方法还包括：

获取所述用户提供的身份识别信息；

建立并存储所述身份识别信息与所述私钥集合之间的关联关系。

4、如权利要求 3 所述的方法，存储加密后的所述私钥集合，具体包括：

在获取到所述用户提供的身份识别信息之后，存储加密后的所述私钥集合。

5、一种调用基于权利要求 1~4 任一项所述的方法存储账户私钥的方法，包括：

私钥管理程序获取所述用户提供的解密密钥；

使用所述解密密钥对加密后的所述私钥集合进行解密；

将解密后的所述私钥集合返回给所述用户。

6、如权利要求 5 所述的方法，在使用所述解密密钥对加密后的所述私钥集合进行解密之前，所述方法还包括：

获取所述用户提供的身份识别信息；

判断所述用户提供的身份识别信息与所述私钥集合所关联的身份识别信息是否匹配；

使用所述解密密钥对加密后的所述私钥集合进行解密，具体包括：

若所述用户提供的身份识别信息与所述私钥集合所关联的身份识别信息匹配，则使用所述解密密钥对加密后的所述私钥集合进行解密；

若所述用户提供的身份识别信息与所述私钥集合所关联的身份识别信息不匹配，则拒绝使用所述解密密钥对加密后的所述私钥集合进行解密。

7、一种存储区块链账户私钥的装置，所述装置安装于用户的用户设备上，所述装置包括：

第一获取模块，获取私钥集合；所述私钥集合包括所述用户注册的区块链账户的至

少一个账户私钥;

第二获取模块, 获取所述用户提供的加密密钥;

加密存储模块, 使用所述加密密钥对所述私钥集合进行加密, 并存储加密后的所述私钥集合。

8、如权利要求 7 所述的装置, 所述私钥集合还包括至少一个其他用户提供给所述用户的账户私钥; 针对每个其他用户, 该其他用户提供给所述用户的账户私钥是该其他用户注册的区块链账户的账户私钥。

9、如权利要求 7 所述的装置, 所述装置还包括:

第三获取模块, 获取所述用户提供的身份识别信息; 建立并存储所述身份识别信息与所述私钥集合之间的关联关系。

10、如权利要求 9 所述的装置, 所述加密存储模块, 在获取到所述用户提供的身份识别信息之后, 存储加密后的所述私钥集合。

11、一种调用基于权利要求 7~10 任一项所述的装置的存储账户私钥的装置, 所述装置安装于用户的用户设备上, 所述装置包括:

获取模块, 获取所述用户提供的解密密钥;

解密模块, 使用所述解密密钥对加密后的所述私钥集合进行解密;

返回模块, 将解密后的所述私钥集合返回给所述用户。

12、如权利要求 11 所述的装置, 所述装置还包括: 身份验证模块, 在使用所述解密密钥对加密后的所述私钥集合进行解密之前, 获取所述用户提供的身份识别信息; 判断所述用户提供的身份识别信息与所述私钥集合所关联的身份识别信息是否匹配;

所述解密模块, 若所述身份验证模块确定所述用户提供的身份识别信息与所述私钥集合所关联的身份识别信息匹配, 则使用所述解密密钥对加密后的所述私钥集合进行解密;

若所述身份验证模块确定所述用户提供的身份识别信息与所述私钥集合所关联的身份识别信息不匹配, 则拒绝使用所述解密密钥对加密后的所述私钥集合进行解密。

13、一种计算机设备, 包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序, 其中, 所述处理器执行所述程序时实现如权利要求 1~6 任一项所述的方法。