

一种存储、调用区块链账户私钥的方法及装置

技术领域

[01] 本说明书实施例涉及信息技术领域，尤其涉及一种存储区块链账户私钥的方法及装置。

背景技术

[02] 在基于区块链网络的服务模式下，用户一般需要在区块链网络中注册区块链账户（或称用户账户），并需要保管自己注册的区块链账户的账户私钥。区块链账户的账户私钥主要用于对区块链账户发起的交易进行签名。

[03] 实践中，用户一般是在自己的本地磁盘中存储自己的区块链账户的账户私钥，需要使用时，再从本地磁盘中获取账户私钥。然而，这种存储账户私钥的方式可靠性较低。

发明内容

[04] 为了解决用户自行保管区块链账户私钥所存在的可靠性较低的问题，本说明书实施例提供一种存储、调用区块链账户私钥的方法及装置，技术方案如下：

[05] 根据本说明书实施例的第 1 方面，提供一种存储区块链账户私钥的方法，包括：

[06] 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；

[07] 获取所述用户提供的加密密钥；

[08] 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。

[09] 根据本说明书实施例的第 2 方面，提供一种调用基于第 1 方面的方法存储的账户私钥的方法，包括：

[10] 私钥管理程序获取所述用户提供的解密密钥；

[11] 使用所述解密密钥对加密后的所述私钥集合进行解密；

[12] 将解密后的所述私钥集合返回给所述用户。

[13] 本说明书实施例所提供的技术方案，在用户的用户设备上安装私钥管理程序。所述私钥管理程序负责对用户的区块链账户私钥进行加密存储。对用户的区块链账户私钥

进行加密所使用的加密密钥是用户指定的。当用户想要使用自己的区块链账户私钥时，需要向私钥管理程序提供所述加密密钥对应的解密密钥，私钥管理程序才能够将解密后的账户私钥提供给用户进行使用。

[14] 通过本说明书实施例，可以实现如下技术效果：

[15] 1、用户不需要记忆自己的账户私钥在磁盘中的存储位置，不会出现找不到自己的账户私钥的情况。由于账户私钥是私钥管理程序负责存储的，用户当需要使用账户私钥时，直接向私钥管理程序请求即可。

[16] 2、私钥管理程序会使用用户指定的加密密钥对账户私钥进行加密。除用户以外的其他人如果无法向私钥管理程序提供所述加密密钥对应的解密密钥，就无法调用用户的账户私钥。

[17] 应当理解的是，以上的一般描述和后文的细节描述仅是示例性和解释性的，并不能限制本说明书实施例。

[18] 此外，本说明书实施例中的任一实施例并不需要达到上述的全部效果。

附图说明

[19] 为了更清楚地说明本说明书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单地介绍，显而易见地，下面描述中的附图仅仅是本说明书实施例中记载的一些实施例，对于本领域普通技术人员来讲，还可以根据这些附图获得其他的附图。

[20] 图1是本说明书实施例提供的一种存储区块链账户私钥的方法的流程示意图；

[21] 图2是本说明书实施例提供的一种调用区块链账户私钥的方法的流程示意图；

[22] 图3是本说明书实施例提供的一种存储区块链账户私钥的装置的结构示意图；

[23] 图4是本说明书实施例提供的一种调用区块链账户私钥的装置的结构示意图；

[24] 图5是用于配置本说明书实施例装置的一种计算机设备的结构示意图。

具体实施方式

[25] 在现有的技术条件下，用户一般自行保管自己的区块链账户密钥。这种保管方式对用户的要求较高，需要用户牢记自己的账户密钥在本地磁盘中的存储位置。此外，如果用户以外的其他人获知了用户的账户密钥在磁盘中的存储位置，则有可能盗用用户的账

户密钥。

[26] 为此，在本说明书实施例中，引入私钥管理程序，将私钥管理程序安装到用户的用户设备上。用户将需要存储的账户私钥提供给私钥管理器负责保管，同时指定一个加密密钥给私钥管理器。私钥管理器是用所述加密密钥对账户私钥进行加密后，存储到用户设备的磁盘中。一方面，加密存储的账户私钥需要一般仅限用户所知的解密密钥进行解密才能使用，另一方面，私钥管理器可以随时应用户的请求从账户私钥的存储位置调出账户私钥，不会出现找不到账户私钥的情况。

[27] 为了使本领域技术人员更好地理解本说明书实施例中的技术方案，下面将结合本说明书实施例中的附图，对本说明书实施例中的技术方案进行详细地描述，显然，所描述的实施例仅仅是本说明书的一部分实施例，而不是全部的实施例。基于本说明书中的实施例，本领域普通技术人员所获得的所有其他实施例，都应当属于保护的范围。

[28] 以下结合附图，详细说明本说明书各实施例提供的技术方案。

[29] 图 1 是本说明书实施例提供的一种存储区块链账户私钥的方法的流程示意图，包括如下步骤：

[30] S100：安装于用户的用户设备上的私钥管理程序获取私钥集合。

[31] 在本说明书实施例中，所述私钥管理器是负责对用户注册的区块链账户的私钥（后文简称为账户私钥）进行保管的程序。

[32] 当用户想要保管自己的账户私钥时，可以打开所述私钥管理程序，将自己的账户私钥输入到所述私钥管理程序。

[33] 需要说明的是，用户的账户私钥的数量可以不止一个。也就是说，私钥管理程序需要对用户输入的包含至少一个账户私钥的私钥集合进行保管。

[34] 进一步地，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。

[35] S102：获取所述用户提供的加密密钥。

[36] 在本说明书实施例中，用户还需要向私钥管理程序输入加密密钥，用于所述自己的账户私钥进行加密。所述加密密钥一般是对称加密密钥，也可以是非对称加密密钥。

[37] S104：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。

[38] 由于所述私钥集合是以加密形式存储于用户设备中的，因此，哪怕所述用户设备由所述用户以外的他人控制，所述私钥集合的明文也难以泄露。

[39] 图 2 是本说明书实施例提供的一种调用区块链账户私钥的方法的流程示意图，包括如下步骤：

[40] S200：私钥管理程序获取所述用户提供的解密密钥。

[41] S202：使用所述解密密钥对加密后的所述私钥集合进行解密。

[42] S204：将解密后的所述私钥集合返回给所述用户。

[43] 需要说明的是，所述解密密钥与前文所述的加密密钥具有对应关系。也就是说，所述解密密钥用于对经过加密密钥加密后的数据进行解密。

[44] 此外，在图 1 所示的方法中，私钥管理程序还可以获取所述用户提供的身份识别信息，然后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。其中，所述身份识别信息是用于识别用户的身份的信息，如用户的手机号、身份证号等。进一步地，所述身份识别信息具体可以是用户的生物识别信息，如指纹信息、人脸信息等。

[45] 具体地，在图 1 所示的方法中，密钥管理程序可以在获取到所述用户提供的身份识别信息之后，再存储加密后的所述私钥集合。也就是说，如果所述用户拒绝向密钥管理程序提供自己的身份识别信息（即拒绝进行实名认证），那么密钥管理器就拒绝存储所述用户提供的私钥集合。

[46] 相应地，在图 2 所示的方法中，密钥管理程序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，可以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。也就是说，密钥管理程序在对存储的私钥集合进行解密之前，需要先确认当前请求获取私钥集合的人是所述私钥集合的拥有者本人。

[47] 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，则密钥管理程序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，则密钥管理程序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。

[48] 由于只有用户本人才能够调用密钥管理程序所保管的账户私钥，因此，哪怕上述

的加密密钥被他人破解，或者上述的加密密钥对应的解密密钥被他人获取，也不会危及用户的账户密钥的安全。

[49] 图 3 是本说明实施例提供的一种存储区块链账户私钥的装置的结构示意图，所述装置安装于用户的用户设备上，所述装置包括：

[50] 第一获取模块 301，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；

[51] 第二获取模块 302，获取所述用户提供的加密密钥；

[52] 加密存储模块 303，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。

[53] 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。

[54] 所述方法还包括：

[55] 第三获取模块 304，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。

[56] 所述加密存储模块 303，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。

[57] 图 4 是本说明书实施例提供的一种调用区块链账户私钥的装置的结构示意图，所述装置安装于用户的用户设备上，所述装置包括：

[58] 获取模块 401，获取所述用户提供的解密密钥；

[59] 解密模块 402，使用所述解密密钥对加密后的所述私钥集合进行解密；

[60] 返回模块 403，将解密后的所述私钥集合返回给所述用户。

[61] 所述装置还包括：身份验证模块 404，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；

[62] 所述解密模块 402，若所述身份验证模块 404 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；

[63] 若所述身份验证模块 404 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。

[64] 本说明书实施例还提供一种计算机设备，其至少包括存储器、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，处理器执行所述程序时实现图 1 或图 2 所示方法的功能。

[65] 图 5 示出了本说明书实施例所提供的一种更为具体的计算设备硬件结构示意图，该设备可以包括：处理器 1410、存储器 1420、输入/输出接口 1430、通信接口 1440 和总线 1450。其中处理器 1410、存储器 1420、输入/输出接口 1430 和通信接口 1440 通过总线 1450 实现彼此之间在设备内部的通信连接。

[66] 处理器 1410 可以采用通用的 CPU（Central Processing Unit，中央处理器）、微处理器、应用专用集成电路（Application Specific Integrated Circuit，ASIC）、或者一个或多个集成电路等方式实现，用于执行相关程序，以实现本说明书实施例所提供的技术方案。

[67] 存储器 1420 可以采用 ROM（Read Only Memory，只读存储器）、RAM（Random Access Memory，随机存取存储器）、静态存储设备，动态存储设备等形式实现。存储器 1420 可以存储操作系统和其他应用程序，在通过软件或者固件来实现本说明书实施例所提供的技术方案时，相关的程序代码保存在存储器 1420 中，并由处理器 1410 来调用执行。

[68] 输入/输出接口 1430 用于连接输入/输出模块，以实现信息输入及输出。输入输出/模块可以作为组件配置在设备中（图中未示出），也可以外接于设备以提供相应功能。其中输入设备可以包括键盘、鼠标、触摸屏、麦克风、各类传感器等，输出设备可以包括显示器、扬声器、振动器、指示灯等。

[69] 通信接口 1440 用于连接通信模块（图中未示出），以实现本设备与其他设备的通信交互。其中通信模块可以通过有线方式（例如 USB、网线等）实现通信，也可以通过无线方式（例如移动网络、WIFI、蓝牙等）实现通信。

[70] 总线 1450 包括一通路，在设备的各个组件（例如处理器 1410、存储器 1420、输入/输出接口 1430 和通信接口 1440）之间传输信息。

[71] 需要说明的是，尽管上述设备仅示出了处理器 1410、存储器 1420、输入/输出接口

1430、通信接口 1440 以及总线 1450，但是在具体实施过程中，该设备还可以包括实现正常运行所必需的其他组件。此外，本领域的技术人员可以理解的是，上述设备中也可以仅包含实现本说明书实施例方案所必需的组件，而不必包含图中所示的全部组件。

[72] 本说明书实施例还提供一种计算机可读存储介质，其上存储有计算机程序，该程序被处理器执行时实现图 1 或图 2 所示方法的功能。

[73] 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、磁带磁磁盘存储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。

[74] 通过以上的实施方式的描述可知，本领域的技术人员可以清楚地了解到本说明书实施例可借助软件加必需的通用硬件平台的方式来实现。基于这样的理解，本说明书实施例的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品可以存储在存储介质中，如 ROM/RAM、磁碟、光盘等，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本说明书实施例各个实施例或者实施例的某些部分所述的方法。

[75] 上述实施例阐明的系统、方法、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。

[76] 本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于方法和设备实施例而言，由于其基本相似于方法实施例，所以描述得比较简单，相关之处参见方法实施例的部分说明即可。以上所描述的方法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，在实施本说明书实施例

方案时可以把各模块的功能在同一个或多个软件和/或硬件中实现。也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实施例方案的目的。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。

[77] 以上所述仅是本说明书实施例的具体实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本说明书实施例原理的前提下，还可以做出若干改进和润饰，这些改进和润饰也应视为本说明书实施例的保护范围。