(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 109727128 B
(45)授权公告日 2020.10.09

(21)申请号 201811493480.4

(22)申请日 2018.12.07

(65)同一申请的已公布的文献号
申请公布号 CN 109727128 A

(43)申请公布日 2019.05.07

(73)专利权人 杭州秘猿科技有限公司
地址 310013 浙江省杭州市西湖区文三路478号华星时代广场A座1301

(72)发明人 王博 曾兵

(74)专利代理机构 北京德崇智捷知识产权代理有限公司 11467
代理人 董柏雷

(51)Int.Cl.
G06Q 40/04(2012.01)
G06Q 20/06(2012.01)
G06Q 20/38(2012.01)

(56)对比文件
CN 108776892 A,2018.11.09
CN 108776892 A,2018.11.09
CN 104811310 A,2015.07.29
CN 102177677 A,2011.09.07
CN 1401171 A,2003.03.05
CN 108830576 A,2018.11.16
US 2018/0077151 A1,2018.03.15
US 8874915 B1,2014.10.28

审查员 李梦芸

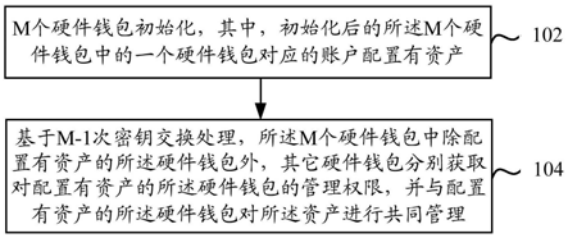
权利要求书2页 说明书9页 附图5页

(54)发明名称

一种基于多个硬件钱包的资产管理方法及系统

(57)摘要

本说明书实施例涉及一种基于多个硬件钱包的资产管理方法及系统，包括：M个硬件钱包初始化，初始化后的M个硬件钱包中的一个硬件钱包对应的账户配置有资产；基于M-1次密钥交换处理，M个硬件钱包中除配置有资产的硬件钱包外，其它硬件钱包分别获取对配置有资产的硬件钱包的管理权限，并与配置有资产的硬件钱包对资产进行共同管理；M为大于等于2的正整数。从而，基于密钥交换技术，使得M个硬件钱包都具有对配置有资产的硬件钱包的管理权限，即实现对硬件钱包的私钥的硬件备份，不需keystore结合密码、或者助记词，保证硬件钱包的安全等级；而且，由于是硬件备份，交付和查看均可以通过硬件实现，及时获取硬件钱包的安全状态。



CN 109727128 B

1.一种基于多个硬件钱包的资产管理方法,包括:

M个硬件钱包初始化,其中,初始化后的所述M个硬件钱包中的一个硬件钱包对应的账户配置有资产;

基于M-1次密钥交换处理,所述M个硬件钱包中除配置有资产的所述硬件钱包外,其它硬件钱包分别获取对配置有资产的所述硬件钱包的管理权限,并与配置有资产的所述硬件钱包对所述资产进行共同管理;具体包括:

基于M-1次密钥交换处理,所述M个硬件钱包中每个硬件钱包都生成相同的共有私钥;

配置有资产的所述硬件钱包利用所述共有私钥对自身的原始私钥进行加密,生成私钥加密结果;

所述M个硬件钱包中除配置有资产的所述硬件钱包外,其它硬件钱包分别基于所述私钥加密结果获取对配置有资产的所述硬件钱包的管理权限;

其中,所述M为大于等于2的正整数。

2.如权利要求1所述的方法,其特征在于,当所述M的取值为2时,基于M-1次密钥交换处理,所述M个硬件钱包中每个硬件钱包都生成相同的共有私钥,具体包括:

基于一次密钥交换处理,两个硬件钱包分别将各自的公钥传输给对方硬件钱包;

两个硬件钱包分别根据自身的原始私钥以及接收到的对方硬件钱包传输来的公钥,生成共有私钥。

3.如权利要求1所述的方法,其特征在于,当所述M的取值为3时,基于M-1次密钥交换处理,所述M个硬件钱包中每个硬件钱包都生成相同的共有私钥,具体包括:

基于第一次密钥交换处理,三个硬件钱包中配置有资产的第一硬件钱包将自身的公钥传输给第二硬件钱包,所述第二硬件钱包将自身的公钥传输给第三硬件钱包,所述第三硬件钱包将自身的公钥传输给所述第一硬件钱包;

所述三个硬件钱包分别根据自身的原始私钥以及接收到的其它硬件钱包传输的公钥,生成各自对应的新私钥;

基于第二次密钥交换处理,所述第一硬件钱包将自身的新私钥传输给所述第二硬件钱包,所述第二硬件钱包将自身的新私钥传输给所述第三硬件钱包,所述第三硬件钱包将自身的新私钥传输给所述第一硬件钱包;

所述三个硬件钱包分别根据自身的原始私钥以及接收到的其它硬件钱包传输的新私钥,生成共有私钥;

或者,

基于第一次密钥交换处理,三个硬件钱包中配置有资产的第一硬件钱包将自身的公钥传输给第三硬件钱包,所述第二硬件钱包将自身的公钥传输给第一硬件钱包,所述第三硬件钱包将自身的公钥传输给所述第二硬件钱包;

所述三个硬件钱包分别根据自身的原始私钥以及接收到的其它硬件钱包传输的公钥,生成各自对应的新私钥;

基于第二次密钥交换处理,所述第一硬件钱包将自身的新私钥传输给所述第三硬件钱包,所述第二硬件钱包将自身的新私钥传输给所述第一硬件钱包,所述第三硬件钱包将自身的新私钥传输给所述第二硬件钱包;

所述三个硬件钱包分别根据自身的原始私钥以及接收到的其它硬件钱包传输的新私

钥,生成共有私钥。

4.如权利要求1所述的方法,其特征在于,其它硬件钱包分别基于所述私钥加密结果获取对配置有资产的所述硬件钱包的管理权限,具体包括:

其它硬件钱包分别利用所述共有私钥对接收到的所述私钥加密结果进行解密,得到配置有资产的所述硬件钱包的原始私钥,以获取对配置有资产的所述硬件钱包的管理权限。

5.如权利要求1-4任一项所述的方法,其特征在于,M个硬件钱包初始化,具体包括:

所述M个硬件钱包分别根据内部随机数生成器生成各自对应的原始私钥;

所述M个硬件钱包分别基于各自对应的原始私钥根据非对称加密算法生成各自对应的公钥;

其中,所述原始私钥不可复制传输。

6.如权利要求1所述的方法,其特征在于,所述M个硬件钱包之间基于生成的共有私钥建立有安全传输信道。

7.如权利要求1所述的方法,其特征在于,所述M个硬件钱包被一个管理者管理;或者,所述M个硬件钱包分别被多个管理者共同管理。

8.一种基于多个硬件钱包的资产管理系统,包括:M个硬件钱包;其中,

所述M个硬件钱包初始化,其中,初始化后的所述M个硬件钱包中的一个硬件钱包对应的账户配置有资产;

基于M-1次密钥交换处理,所述M个硬件钱包中除配置有资产的所述硬件钱包外,其它硬件钱包分别获取对配置有资产的所述硬件钱包的管理权限,并与配置有资产的所述硬件钱包对所述资产进行共同管理;所述M个硬件钱包具体用于:

基于M-1次密钥交换处理,生成相同的共有私钥;

配置有资产的所述硬件钱包,具体用于:利用所述共有私钥对自身的原始私钥进行加密,生成私钥加密结果;

所述M个硬件钱包中除配置有资产的所述硬件钱包外,其它硬件钱包,具体用于:分别基于所述私钥加密结果获取对配置有资产的所述硬件钱包的管理权限;

其中,所述M为大于等于2的正整数。

一种基于多个硬件钱包的资产管理方法及系统

技术领域

[0001] 本说明书实施例涉及区块链网络技术领域，尤其涉及一种基于多个硬件钱包的资产管理方法及系统。

背景技术

[0002] 区块链中电子钱包主要用于管理区块链上账户的数字资产，电子钱包(可理解为硬件钱包)的账户安全由私钥和公钥共同维护。即每个电子钱包的账户包含一份密钥对，也就是私钥与公钥。当该电子钱包(对应的账户)发生交易时，每笔交易都需要一个有效的数字签名才会被存储在区块链，以实现交易。而在交易过程中，只有有效的私钥才能产生有效的数字签名，因此，获知电子钱包的账户私钥就拥有了对该账户的管理支配权。

[0003] 为了防止别人盗取私钥而获取该账户的管理支配权，或者防止自己丢失私钥而丧失对该账户的管理支配权，可以对电子钱包备份，具体可以是对电子钱包的私钥进行备份。由于私钥是一串随机生成的256位二进制数字，不方便用户保存或者记录，所以，会使用keystore与密码结合的方式，或者，助记词的方式来保存私钥。其中，keystore与密码结合的方式：是将私钥与公钥以加密(创建电子钱包时会设置的密码password)的方式保存为一份JSON文件，这份JSON文件就是keystore，所以这种保存私钥的方式需要同时备份keystore和对应的password；而助记词的方式：是通过随机生成12～24个容易记住的单词序列，即助记词，该单词序列和私钥有相关性。

[0004] 硬件钱包虽然安全性高、可靠性高、具有实体方便管理等优势，但目前的私钥备份方法(keystore与密码结合的方式，或者，助记词的方式)均存在很大风险，容易丢失，被盗，无法有效保证硬件钱包的安全等级。

发明内容

[0005] 本说明书实施例提供一种基于多个硬件钱包的资产管理方法及系统，用以解决现有技术中私钥备份无法保证硬件钱包账户安全的问题。

[0006] 为了解决上述技术问题，本说明书实施例采用下述技术方案：

[0007] 第一方面，提供了一种基于多个硬件钱包的资产管理方法，包括：

[0008] M个硬件钱包初始化，其中，初始化后的所述M个硬件钱包中的一个硬件钱包对应的账户配置有资产；

[0009] 基于M-1次密钥交换处理，所述M个硬件钱包中除配置有资产的所述硬件钱包外，其它硬件钱包分别获取对配置有资产的所述硬件钱包的管理权限，并与配置有资产的所述硬件钱包对所述资产进行共同管理；

[0010] 其中，所述M为大于等于2的正整数。

[0011] 第二方面，提供了一种基于多个硬件钱包的资产管理系统，包括：M个硬件钱包；其中，

[0012] 所述M个硬件钱包初始化，其中，初始化后的所述M个硬件钱包中的一个硬件钱包

对应的账户配置有资产；

[0013] 基于M-1次密钥交换处理，所述M个硬件钱包中除配置有资产的所述硬件钱包外，其它硬件钱包分别获取对配置有资产的所述硬件钱包的管理权限，并与配置有资产的所述硬件钱包对所述资产进行共同管理；

[0014] 其中，所述M为大于等于2的正整数。

[0015] 本说明书实施例采用的上述至少一个技术方案能够达到以下有益效果：

[0016] 在本说明书实施例中，基于密钥交换技术，使得M个硬件钱包都具有对配置有资产的硬件钱包的管理权限，即实现对硬件钱包的私钥的硬件备份，不需keystore结合密码、或者助记词文件，保证硬件钱包的安全等级；而且，由于是通过硬件备份，交付和查看均可以通过硬件实现，可以及时获取硬件钱包的安全状态，即查看是否被盗或资产是否被转移。此外，硬件钱包的私钥备份过程中不会向外界泄露信息，保证私钥备份操作安全；以及，还可以通过多个硬件钱包的分配，实现账户的多人共享，共同管理。

附图说明

[0017] 为了更清楚地说明本说明书实施例或现有技术中的技术方案，下面将对实施例或现有技术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，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[0018] 图1为本说明书实施例提供的一种基于多个硬件钱包的资产管理方法步骤示意图；；

[0019] 图2为本说明书实施例中步骤104的具体步骤示意图；

[0020] 图3a-图3c分别为本说明书实施例提供的基于多个硬件钱包的资产管理流程示意图；

[0021] 图4为本说明书实施例提供的基于多个硬件钱包的资产管理系统的结构示意图；

[0022] 图5为本说明书实施例提供的电子设备的结构示意图。

具体实施方式

[0023] 为使本说明书实施例的目的、技术方案和优点更加清楚，下面将结合本说明书具体实施例及相应的附图对本说明书实施例的技术方案进行清楚、完整地描述。显然，所描述的实施例仅是本说明书一部分实施例，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在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本说明书实施例保护的范围。

[0024] 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。

[0025] 实施例一

[0026] 参照图1所示，为本说明书实施例提供的一种基于多个硬件钱包的资产管理方法，该资产管理方法可以应用于区块链网络技术中的账户资产管理，具体使用场景可以是基于多个硬件钱包实现的对相应账户中资产的管理。需要说明的是，本说明书实施例中，资产管理的具体管理内容并不是作为保护重点，而是在于如何基于多个硬件钱包实现对区块链中相应账户上的资产的安全管理。

[0027] 本说明书实施例中,所述资产管理方法可以包括以下步骤:

[0028] 步骤102:M个硬件钱包初始化,其中,初始化后的所述M个硬件钱包中的一个硬件钱包对应的账户配置有资产。

[0029] 考虑到现有技术中是通过硬件钱包结合软件备份的方式,实现对硬件钱包的私钥备份,这种方式存在较多局限性以及不安全因素。而本说明书改变了现有的私钥备份方式,并不通过keystore与密码结合,或者,助记词等软件备份方式对私钥进行备份,而是通过多个硬件钱包之间相互备份的纯硬件备份方式,实现对硬件钱包的私钥备份。

[0030] 应理解,本说明书中M个硬件钱包初始化的过程,即是M个硬件钱包分别生成私钥-公钥等初始化的过程。具体地,该步骤102可执行为:

[0031] 所述M个硬件钱包分别根据内部随机数生成器生成各自对应的原始私钥;

[0032] 所述M个硬件钱包分别基于各自对应的原始私钥根据非对称加密算法生成各自对应的公钥;

[0033] 其中,所述原始私钥不可复制传输。换言之,每个硬件钱包的原始私钥都是不可由外界导入或是导出外界的,即不可直接传输给其它装置,例如其它硬件钱包。

[0034] 应理解,所述原始私钥(以k表示)是一串数字,是根据每个硬件钱包的内部随机数生成器随机生成的。基于所述原始私钥,硬件钱包可以使用非对称加密算法这类算法中的单向加密函数生成一个公钥(以K表示)。在生成公钥后,就可以使用单向加密哈希函数生成该硬件钱包的账户地址。其中,每个硬件钱包的原始私钥和公钥的结构关系可以为:原始私钥:a;公钥:aG,其中,G可以理解为单向加密函数。

[0035] 原始私钥与公钥是通过非对称加密算法生成,非对称加密算法有很多种类,本说明书实施例可以采用椭圆曲线算法,其实也不限于采用其它非对称加密算法,本说明书不做赘述。

[0036] 步骤104:基于M-1次密钥交换处理,所述M个硬件钱包中除配置有资产的所述硬件钱包外,其它硬件钱包分别获取对配置有资产的所述硬件钱包的管理权限,并与配置有资产的所述硬件钱包对所述资产进行共同管理。

[0037] 其中,所述M为大于等于2的正整数。

[0038] 在该步骤中,M个硬件钱包之间,利用密钥交换技术,进行M-1次密钥交换处理,这样,除了配置有资产的硬件钱包本身就具有对自身账户资产的管理权限这种情况外,其它硬件钱包也分别都可以获取到对配置有资产的硬件钱包的管理权限,这样,可以与配置有资产的硬件钱包对资产进行共同管理。

[0039] 在本说明书实施例中,基于密钥交换技术,使得M个硬件钱包都具有对配置有资产的硬件钱包的管理权限,即实现对硬件钱包的私钥的硬件备份,不需keystore结合密码、或者助记词文件,保证硬件钱包的安全等级;而且,由于是通过硬件备份,交付和查看均可以通过硬件实现,可以及时获取硬件钱包的安全状态,即查看是否被盗或资产是否被转移。

[0040] 一种可实现的方案,参照图2所示,步骤104具体执行为:

[0041] 步骤202:基于M-1次密钥交换处理,所述M个硬件钱包中每个硬件钱包都生成相同的共有私钥。

[0042] 应理解,在该步骤中,每个硬件钱包都会基于密钥交换处理的结果,生成一个共有私钥,而这M个硬件钱包各自生成的共有私钥都是相同的。

[0043] 其中，每个硬件钱包对应的共有私钥的表现形式可能不同，但是实质内容是相同的，后续通过具体的实例进行解释。

[0044] --当所述M的取值为2时，步骤202可以具体执行为：

[0045] 基于一次密钥交换处理，两个硬件钱包分别将各自的公钥传输给对方硬件钱包；

[0046] 两个硬件钱包分别根据自身的原始私钥以及接收到的对方硬件钱包传输来的公钥，生成共有私钥。

[0047] --当所述M的取值为3时，步骤202可以具体执行为：

[0048] 基于第一次密钥交换处理，三个硬件钱包中配置有资产的第一硬件钱包将自身的公钥传输给第二硬件钱包，所述第二硬件钱包将自身的公钥传输给第三硬件钱包，所述第三硬件钱包将自身的公钥传输给所述第一硬件钱包；

[0049] 所述三个硬件钱包分别根据自身的原始私钥以及接收到的其它硬件钱包传输的公钥，生成各自对应的新私钥；

[0050] 基于第二次密钥交换处理，所述第一硬件钱包将自身的新私钥传输给所述第二硬件钱包，所述第二硬件钱包将自身的新私钥传输给所述第三硬件钱包，所述第三硬件钱包将自身的新私钥传输给所述第一硬件钱包；

[0051] 所述三个硬件钱包分别根据自身的原始私钥以及接收到的其它硬件钱包传输的新私钥，生成共有私钥。

[0052] 或者，

[0053] 基于第一次密钥交换处理，三个硬件钱包中配置有资产的第一硬件钱包将自身的公钥传输给第三硬件钱包，所述第二硬件钱包将自身的公钥传输给第一硬件钱包，所述第三硬件钱包将自身的公钥传输给所述第二硬件钱包；

[0054] 所述三个硬件钱包分别根据自身的原始私钥以及接收到的其它硬件钱包传输的公钥，生成各自对应的新私钥；

[0055] 基于第二次密钥交换处理，所述第一硬件钱包将自身的新私钥传输给所述第三硬件钱包，所述第二硬件钱包将自身的新私钥传输给所述第一硬件钱包，所述第三硬件钱包将自身的新私钥传输给所述第二硬件钱包；

[0056] 所述三个硬件钱包分别根据自身的原始私钥以及接收到的其它硬件钱包传输的新私钥，生成共有私钥。

[0057] 步骤204：配置有资产的所述硬件钱包利用所述共有私钥对自身的原始私钥进行加密，生成私钥加密结果。

[0058] 应理解，配置有资产的硬件钱包可以使用生成的共有私钥对自身的原始私钥进行加密，生成私钥加密结果，该私钥加密结果实质上是基于共有私钥和原始私钥加密后生成的所属配置有资产的硬件钱包的最终私钥，该最终私钥中携带有被加密处理的原始私钥，因此，可以将该最终私钥传输给其它硬件钱包。其中，使用生成的共有私钥对自身的原始私钥进行加密时，具体可以使用现有的非对称加密算法，本说明书并不对此进行限定。

[0059] 步骤206：所述M个硬件钱包中除配置有资产的所述硬件钱包外，其它硬件钱包分别基于所述私钥加密结果获取对配置有资产的所述硬件钱包的管理权限。

[0060] 一种可实现的方案，步骤206可具体执行为：其它硬件钱包分别利用所述共有私钥对接收到的所述私钥加密结果进行解密，得到配置有资产的所述硬件钱包的原始私钥，以

获取对配置有资产的所述硬件钱包的管理权限。

[0061] 其实,在本说明书实施例中,所述M个硬件钱包之间基于生成的共有私钥建立有安全传输信道。这是因为,在M个硬件钱包基于密钥交换技术,分别生成相同的共有私钥后,其实就相当于这M个硬件钱包之间可以基于该相同的共有私钥进行加解密处理,那么,就相当于是建立了安全的传输信道。从而,硬件钱包的原始私钥的备份过程中不会向外界泄露信息,保证原始私钥的备份安全以及资产安全。

[0062] 可选地,在本说明书实施例中,所述M个硬件钱包可以被一个管理者管理;或者,所述M个硬件钱包可以分别被多个管理者共同管理。由此,通过多个硬件钱包的分配,可实现账户的多用户共享,同时共同管理。

[0063] 也就是说,可以是一个用户同时掌管着这M个硬件钱包,在配置有资产的硬件钱包的资产存在交易时,如果M个硬件钱包都在这一个用户的掌控范围内,那么,说明该硬件钱包没有被盗,仍是安全的。如果M个硬件钱包中至少一个不在这一个用户的掌控范围内,即脱离了该用户的掌控,那么,说明该硬件钱包存在被盗风险。也可以是多个用户分别掌管着这M个硬件钱包,在配置有资产的硬件钱包的资产存在交易时,如果M个硬件钱包分别在各自所属用户的掌控范围内,那么,说明该硬件钱包没有被盗,仍是安全的。如果M个硬件钱包中至少一个不在各自所属用户的掌控范围内,即脱离了所属用户的掌控,那么,说明该硬件钱包存在被盗风险。

[0064] 下面通过两个具体的实例对本说明书方案进行详述。

[0065] --基于两个硬件钱包对资产进行管理(硬件钱包1对应的账户配置有资产)

[0066] 首先,参照图3a所示,对硬件钱包1和硬件钱包2分别进行初始化操作。其中,硬件钱包1根据自身的内部随机数生成器生成原始私钥sk1(a),并利用该私钥sk1(a)生成公钥pk1(aG);同理,硬件钱包2根据自身的内部随机数生成器生成原始私钥sk2(b),并利用该私钥sk2(b)生成公钥pk2(bG)。

[0067] 然后,利用密钥交换技术,硬件钱包1将自身的公钥pk1(aG)传输给硬件钱包2;同时,硬件钱包2将自身的公钥pk2(bG)传输给硬件钱包1。

[0068] 硬件钱包1根据自身的原始私钥sk1(a)与接收到的硬件钱包2传输来的公钥pk2(bG),生成新的私钥sk1’(abG);硬件钱包2根据自身的原始私钥sk2(b)与接收到的硬件钱包1传输来的公钥pk1(aG),生成新的私钥sk2’(abG)。其中,硬件钱包1生成的新的私钥sk1’(abG)与硬件钱包2生成的新的私钥sk2’(abG)相同,从而,基于该相同的共有私钥建立出较为安全的传输信道。

[0069] 硬件钱包1使用共有私钥sk1’(abG)对自身的原始私钥sk1(a)进行加密,得到xk1,并把这个私钥加密结果传输给硬件钱包2。

[0070] 硬件钱包2使用共有私钥sk2’(abG)对接收到的私钥加密结果xk1进行解密,从而得到硬件钱包1的原始私钥sk1(a),进而,硬件钱包2获取到对硬件钱包1对应的账户上资产的支配管理权限。

[0071] 上述资产管理方案中,仅通过一次密钥交换处理,就可以基于两个硬件钱包实现对其中一个配置有资产的硬件钱包的原始私钥的硬件备份,避免通过现有技术中软件备份造成的丢失、被盗等问题,提升硬件钱包的私钥备份安全性,以及对硬件钱包的资产管理的安全性。

[0072] --基于三个硬件钱包对资产进行管理

[0073] 参照图3b所示，对硬件钱包1、硬件钱包2和硬件钱包3分别进行初始化操作。其中，硬件钱包1根据自身的内部随机数生成器生成原始私钥sk1(a)，并利用该私钥sk1(a)生成公钥pk1(aG)；同理，硬件钱包2根据自身的内部随机数生成器生成原始私钥sk2(b)，并利用该私钥sk2(b)生成公钥pk2(bG)；硬件钱包3根据自身的内部随机数生成器生成原始私钥sk3(c)，并利用该私钥sk3(c)生成公钥pk3(cG)。

[0074] 然后，利用第一次密钥交换技术，硬件钱包1将自身的公钥pk1(aG)传输给硬件钱包2；同时，硬件钱包2将自身的公钥pk2(bG)传输给硬件钱包3；硬件钱包3将自身的公钥pk3(cG)传输给硬件钱包1。

[0075] 硬件钱包1根据自身的原始私钥sk1(a)与接收到的硬件钱包3传输来的公钥pk3(cG)，生成新的私钥sk1’(acG)；硬件钱包2根据自身的原始私钥sk2(b)与接收到的硬件钱包1传输来的公钥pk1(aG)，生成新的私钥sk2’(abG)；硬件钱包3根据自身的原始私钥sk3(c)与接收到的硬件钱包2传输来的公钥pk2(bG)，生成新的私钥sk3’(bcG)。

[0076] 接着，再利用第二次密钥交换技术，硬件钱包1将新的私钥sk1’(acG)传输给硬件钱包2；同时，硬件钱包2将新的私钥sk2’(abG)传输给硬件钱包3；硬件钱包3将新的私钥sk3’(bcG)传输给硬件钱包1。

[0077] 硬件钱包1根据自身的原始私钥sk1(a)与接收到的硬件钱包3传输来的新的私钥sk3’(bcG)，生成最终私钥sk1”(abcG)；硬件钱包2根据自身的原始私钥sk2(b)与接收到的硬件钱包1传输来的新的私钥sk1’(acG)，生成最终私钥sk2”(abcG)；硬件钱包3根据自身的原始私钥sk3(c)与接收到的硬件钱包2传输来的新的私钥sk2’(abG)，生成最终私钥sk3”(abcG)。其中，硬件钱包1生成的最终私钥sk1”(abcG)与硬件钱包2生成的最终私钥sk2”(abcG)以及硬件钱包3生成的最终私钥sk3”(abcG)相同，从而，基于该相同的共有私钥建立出较为安全的传输信道。

[0078] 硬件钱包1使用共有私钥sk1”(abcG)对自身的原始私钥sk1(a)进行加密，得到yk1，并把这个私钥加密结果分别传输给硬件钱包2和硬件钱包3。

[0079] 硬件钱包2使用共有私钥sk2”(abcG)对接收到的私钥加密结果yk1进行解密，从而得到硬件钱包1的原始私钥sk1(a)；硬件钱包3使用共有私钥sk3”(abcG)对接收到的私钥加密结果yk1进行解密，从而得到硬件钱包1的原始私钥sk1(a)；进而，硬件钱包2和硬件钱包3分别获取到对硬件钱包1对应的账户上资产的支配管理权限。

[0080] 或者，

[0081] 参照图3c所示，对硬件钱包1、硬件钱包2和硬件钱包3分别进行初始化操作。其中，硬件钱包1根据自身的内部随机数生成器生成原始私钥sk1(a)，并利用该私钥sk1(a)生成公钥pk1(aG)；同理，硬件钱包2根据自身的内部随机数生成器生成原始私钥sk2(b)，并利用该私钥sk2(b)生成公钥pk2(bG)；硬件钱包3根据自身的内部随机数生成器生成原始私钥sk3(c)，并利用该私钥sk3(c)生成公钥pk3(cG)。

[0082] 然后，利用第一次密钥交换技术，硬件钱包1将自身的公钥pk1(aG)传输给硬件钱包3；同时，硬件钱包2将自身的公钥pk2(bG)传输给硬件钱包1；硬件钱包3将自身的公钥pk3(cG)传输给硬件钱包2。

[0083] 硬件钱包1根据自身的原始私钥sk1(a)与接收到的硬件钱包2传输来的公钥pk2

(bG)，生成新的私钥sk1’(abG)；硬件钱包2根据自身的原始私钥sk2(b)与接收到的硬件钱包3传输来的公钥pk3(cG)，生成新的私钥sk2’(bcG)；硬件钱包3根据自身的原始私钥sk3(c)与接收到的硬件钱包1传输来的公钥pk1(aG)，生成新的私钥sk3’(acG)。

[0084] 接着，再利用第二次密钥交换技术，硬件钱包1将新的私钥sk1’(abG)传输给硬件钱包3；同时，硬件钱包2将新的私钥sk2’(bcG)传输给硬件钱包1；硬件钱包3将新的私钥sk3’(acG)传输给硬件钱包2。

[0085] 硬件钱包1根据自身的原始私钥sk1(a)与接收到的硬件钱包2传输来的新的私钥sk2’(bcG)，生成最终私钥sk1”(abcG)；硬件钱包2根据自身的原始私钥sk2(b)与接收到的硬件钱包3传输来的新的私钥sk3’(acG)，生成最终私钥sk2”(abcG)；硬件钱包3根据自身的原始私钥sk3(c)与接收到的硬件钱包1传输来的新的私钥sk1’(abG)，生成最终私钥sk3”(abcG)。其中，硬件钱包1生成的最终私钥sk1”(abcG)与硬件钱包2生成的最终私钥sk2”(abcG)以及硬件钱包3生成的最终私钥sk3”(abcG)相同，从而，基于该相同的共有私钥建立出较为安全的传输信道。

[0086] 硬件钱包1使用共有私钥sk1”(abcG)对自身的原始私钥sk1(a)进行加密，得到yk1，并把这个私钥加密结果分别传输给硬件钱包2和硬件钱包3。

[0087] 硬件钱包2使用共有私钥sk2”(abcG)对接收到的私钥加密结果yk1进行解密，从而得到硬件钱包1的原始私钥sk1(a)；硬件钱包3使用共有私钥sk3”(abcG)对接收到的私钥加密结果yk1进行解密，从而得到硬件钱包1的原始私钥sk1(a)；进而，硬件钱包2和硬件钱包3分别获取到对硬件钱包1对应的账户上资产的支配管理权限。

[0088] 上述资产管理方案中，通过两次密钥交换处理，可以基于三个硬件钱包实现对其中一个配置有资产的硬件钱包的原始私钥的硬件备份，避免通过现有技术中软件备份造成的丢失、被盗等问题，提升硬件钱包的私钥备份安全性，以及对硬件钱包的资产管理的安全性。

[0089] 需要说明的是，在图3a-图3c各图中，定义“+”号表示两个密钥之间进行加密处理，“-”号表示两个密钥之间进行解密处理。

[0090] 实施例二

[0091] 参照图4所示，为本说明书实施例提供的基于多个硬件钱包的资产管理系统的结构示意图，该系统包括：M个硬件钱包402；其中，

[0092] 所述M个硬件钱包402初始化，其中，初始化后的所述M个硬件钱包402中的一个硬件钱包402对应的账户配置有资产；

[0093] 基于M-1次密钥交换处理，所述M个硬件钱包402中除配置有资产的所述硬件钱包402外，其它硬件钱包402分别获取对配置有资产的所述硬件钱包402的管理权限，并与配置有资产的所述硬件钱包402对所述资产进行共同管理；

[0094] 其中，所述M为大于等于2的正整数。

[0095] 在本说明书实施例中，基于密钥交换技术，使得M个硬件钱包都具有对配置有资产的硬件钱包的管理权限，即实现对硬件钱包的私钥的硬件备份，不需keystore结合密码、或者助记词文件，保证硬件钱包的安全等级；而且，由于是通过硬件备份，交付和查看均可以通过硬件实现，可以及时获取硬件钱包的安全状态，即查看是否被盗或资产是否被转移。

[0096] 可选地，作为一个实施例，所述M个硬件钱包402具体用于：基于M-1次密钥交换处

理,生成相同的共有私钥;

[0097] 配置有资产的所述硬件钱包402,具体用于:利用所述共有私钥对自身的原始私钥进行加密,生成私钥加密结果;

[0098] 所述M个硬件钱包402中除配置有资产的所述硬件钱包402外,其它硬件钱包402,具体用于:分别基于所述私钥加密结果获取对配置有资产的所述硬件钱包的管理权限。

[0099] 应理解,本说明书实施例的基于多个硬件钱包的资产管理系统还可执行图1-图3b中的方法,并实现在图1-图3b所示实施例的功能,在此不再赘述。

[0100] 实施例三

[0101] 下面参照图5详细介绍本说明书实施例的电子设备,该电子设备具体可以是硬件钱包。请参考图5,在硬件层面,该电子设备包括处理器,可选地还包括内部总线、网络接口、存储器。其中,存储器可能包含内存,例如高速随机存取存储器(Random-Access Memory,RAM),也可能还包括非易失性存储器(Non-Volatile Memory),例如至少1个磁盘存储器等。当然,该电子设备还可能包括其他业务所需要的硬件。

[0102] 处理器、网络接口和存储器可以通过内部总线相互连接,该内部总线可以是工业标准体系结构(Industry Standard Architecture,ISA)总线、外设部件互连标准(Peripheral Component Interconnect,PCI)总线或扩展工业标准结构(Extended Industry Standard Architecture,EISA)总线等。所述总线可以分为地址总线、数据总线、控制总线等。为便于表示,图5中仅用一个双向箭头表示,但并不表示仅有一根总线或一种类型的总线。

[0103] 存储器,用于存放程序。具体地,程序可以包括程序代码,所述程序代码包括计算机操作指令。存储器可以包括内存和非易失性存储器,并向处理器提供指令和数据。

[0104] 处理器从非易失性存储器中读取对应的计算机程序到内存中然后运行,在逻辑层面上形成硬件钱包。处理器,执行存储器所存放的程序,并具体用于执行前文所述电子设备作为执行主体时所执行的方法操作。

[0105] 上述如本说明书实施例图1-图3b所示实施例揭示的方法可以应用于处理器中,或者由处理器实现。处理器可能是一种集成电路芯片,具有信号的处理能力。在实现过程中,上述方法的各步骤可以通过处理器中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器可以是通用处理器,包括中央处理器(Central Processing Unit,CPU)、网络处理器(Network Processor,NP)等;还可以是数字信号处理器(Digital Signal Processor,DSP)、专用集成电路(Application Specific Integrated Circuit,ASIC)、现场可编程门阵列(Field—Programmable Gate Array,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说明书实施例中的公开的各方法、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。结合本说明书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。该存储介质位于存储器,处理器读取存储器中的信息,结合其硬件完成上述方法的步骤。

[0106] 该电子设备还可执行图1-图3b的方法,并实现硬件钱包在图1-图3b所示实施例的

功能，本说明书实施例在此不再赘述。

[0107] 当然，除了软件实现方式之外，本说明书实施例的电子设备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。

[0108] 实施例四

[0109] 本说明书实施例还提供一种计算机可读存储介质，所述计算机可读存储介质存储一个或多个程序，所述一个或多个程序当被包括多个应用程序的电子设备执行时，使得所述电子设备作为执行主体时所执行的方法操作

[0110] 其中，所述的计算机可读存储介质，如只读存储器(Read-Only Memory，ROM)、随机存取存储器(Random Access Memory，RAM)、磁碟或者光盘等。

[0111] 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，对于系统实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[0112] 以上所述仅为本申请的实施例而已，并不用于限制本申请。对于本领域技术人员来说，本申请可以有各种更改和变化。凡在本申请的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在本申请的权利要求范围之内。

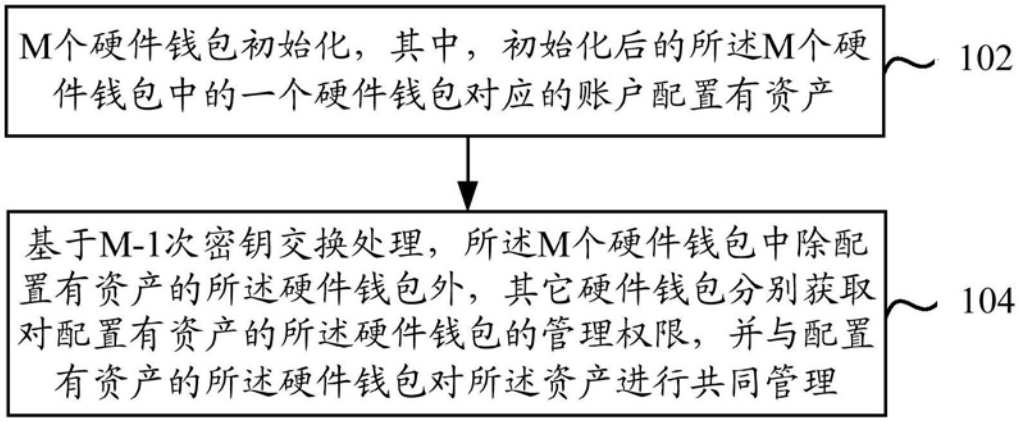

M个硬件钱包初始化，其中，初始化后的所述M个硬件钱包中的一个硬件钱包对应的账户配置有资产
102
基于M-1次密钥交换处理，所述M个硬件钱包中除配置有资产的所述硬件钱包外，其它硬件钱包分别获取对配置有资产的所述硬件钱包的管理权限，并与配置有资产的所述硬件钱包对所述资产进行共同管理
104

图1

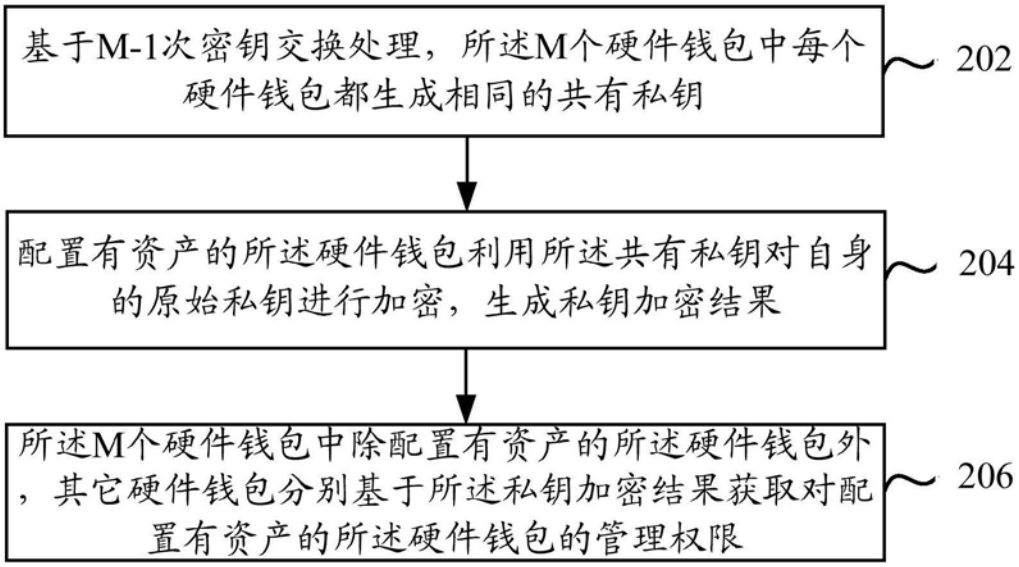

基于M-1次密钥交换处理，所述M个硬件钱包中每个硬件钱包都生成相同的共有私钥
202
配置有资产的所述硬件钱包利用所述共有私钥对自身的原始私钥进行加密，生成私钥加密结果
204
所述M个硬件钱包中除配置有资产的所述硬件钱包外，其它硬件钱包分别基于所述私钥加密结果获取对配置有资产的所述硬件钱包的管理权限
206

图2

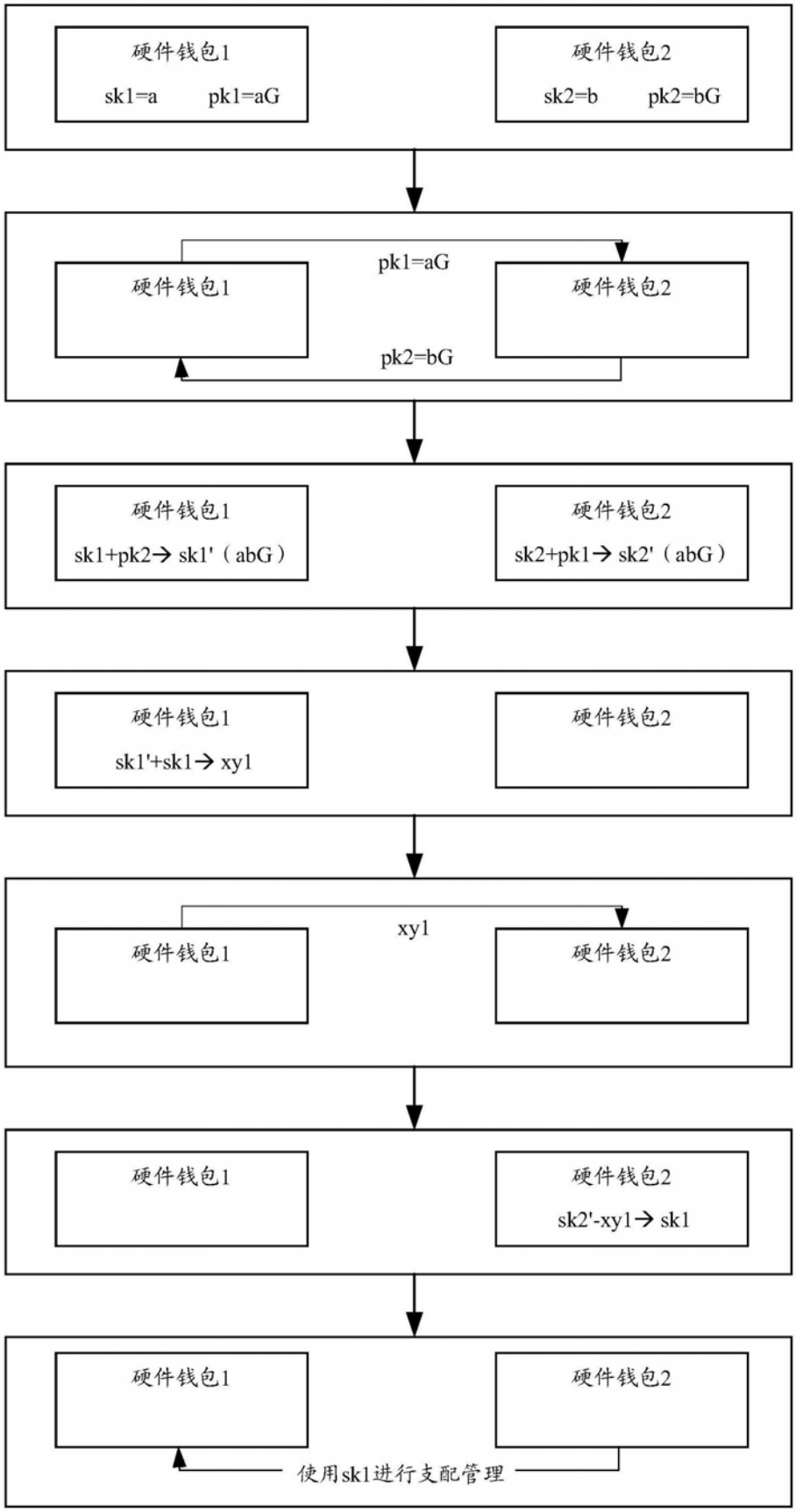

硬件钱包1
sk1=a pk1=aG
硬件钱包2
sk2=b pk2=bG
pk1=aG
硬件钱包1
硬件钱包2
pk2=bG
硬件钱包1
sk1+pk2→ sk1'（abG）
硬件钱包2
sk2+pk1→ sk2'（abG）
硬件钱包1
sk1'+sk1→ xy1
硬件钱包2
xy1
硬件钱包1
硬件钱包2
硬件钱包1
硬件钱包2
sk2'-xy1→ sk1
硬件钱包1
硬件钱包2
使用sk1进行支配管理

图3a

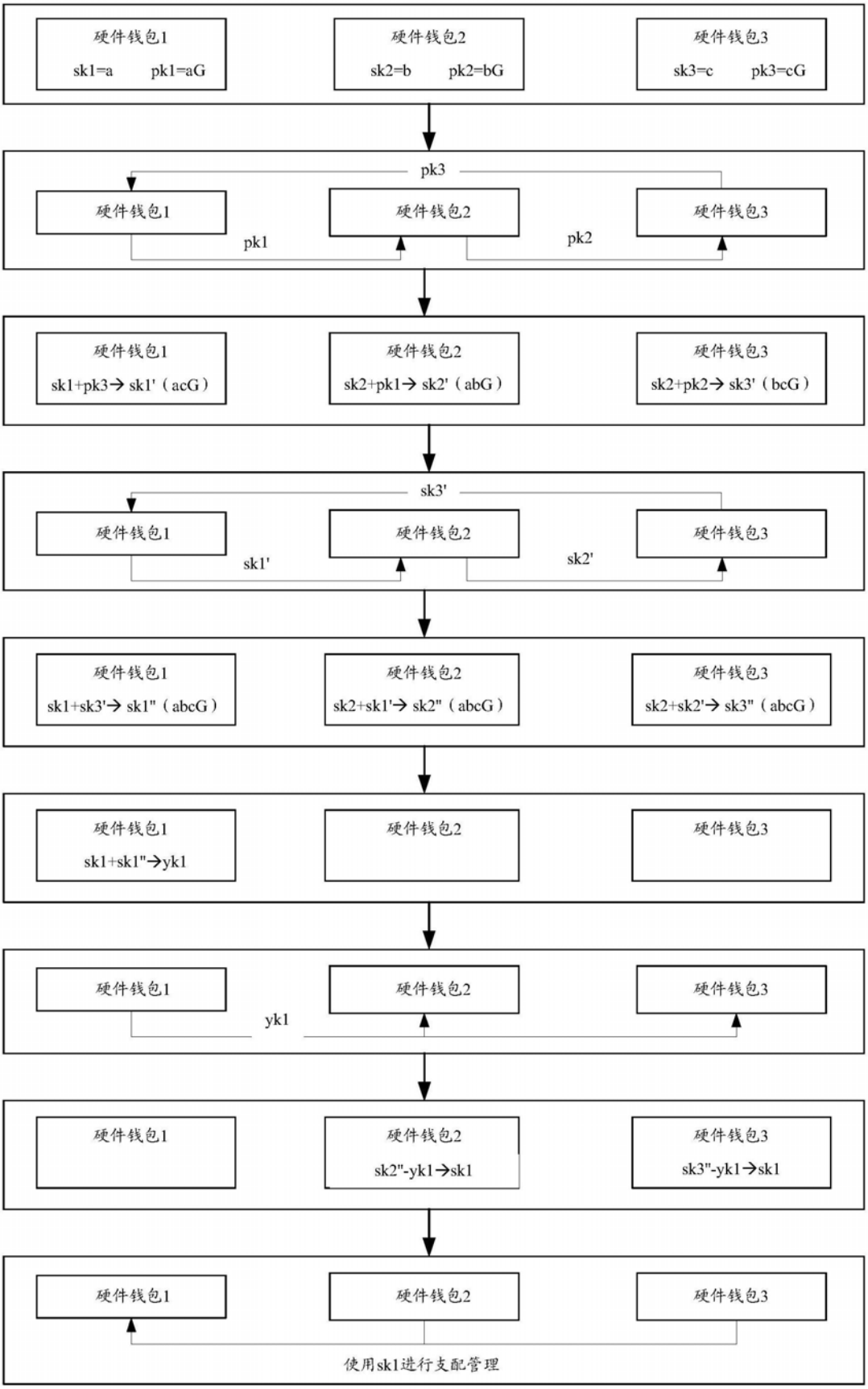

硬件钱包1
sk1=a pk1=aG
硬件钱包2
sk2=b pk2=bG
硬件钱包3
sk3=c pk3=cG
pk3
硬件钱包1
硬件钱包2
硬件钱包3
pk1
pk2
硬件钱包1
sk1+pk3→ sk1'（acG）
硬件钱包2
sk2+pk1→ sk2'（abG）
硬件钱包3
sk2+pk2→ sk3'（bcG）
sk3'
硬件钱包1
硬件钱包2
硬件钱包3
sk1'
sk2'
硬件钱包1
sk1+sk3'→ sk1"（abcG）
硬件钱包2
sk2+sk1'→ sk2"（abcG）
硬件钱包3
sk2+sk2'→ sk3"（abcG）
硬件钱包1
sk1+sk1"→yk1
硬件钱包2
硬件钱包3
硬件钱包1
硬件钱包2
硬件钱包3
yk1
硬件钱包1
硬件钱包2
sk2"-yk1→sk1
硬件钱包3
sk3"-yk1→sk1
硬件钱包1
硬件钱包2
硬件钱包3
使用sk1进行支配管理

图3b

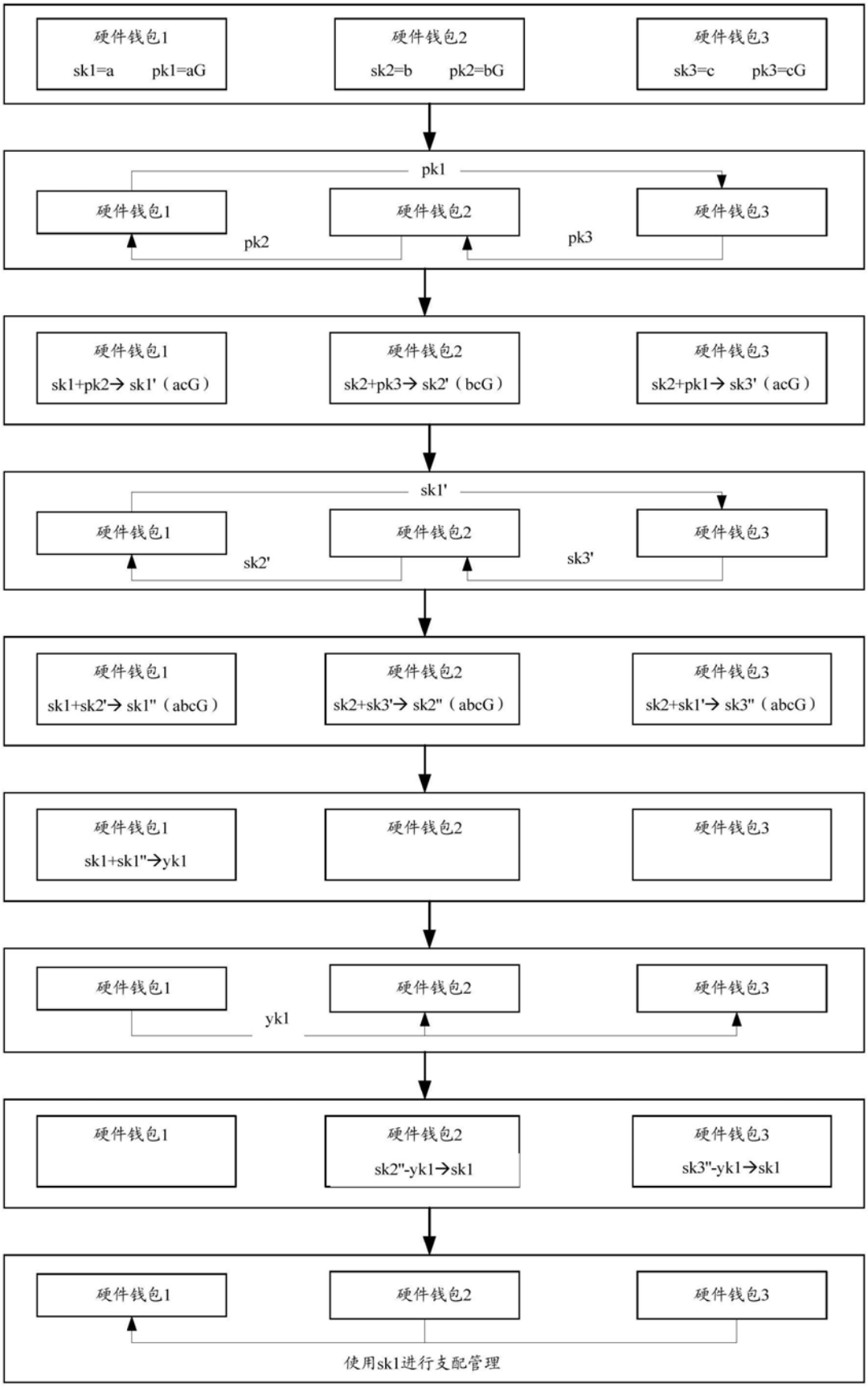

硬件钱包1
sk1=a pk1=aG
硬件钱包2
sk2=b pk2=bG
硬件钱包3
sk3=c pk3=cG
pk1
硬件钱包1
硬件钱包2
硬件钱包3
pk2
pk3
硬件钱包1
sk1+pk2→ sk1'（acG）
硬件钱包2
sk2+pk3→ sk2'（bcG）
硬件钱包3
sk2+pk1→ sk3'（acG）
sk1'
硬件钱包1
硬件钱包2
硬件钱包3
sk2'
sk3'
硬件钱包1
sk1+sk2'→ sk1''（abcG）
硬件钱包2
sk2+sk3'→ sk2''（abcG）
硬件钱包3
sk2+sk1'→ sk3''（abcG）
硬件钱包1
sk1+sk1''→yk1
硬件钱包2
硬件钱包3
硬件钱包1
硬件钱包2
硬件钱包3
yk1
硬件钱包1
硬件钱包2
sk2''-yk1→sk1
硬件钱包3
sk3''-yk1→sk1
硬件钱包1
硬件钱包2
硬件钱包3
使用sk1进行支配管理

图3c

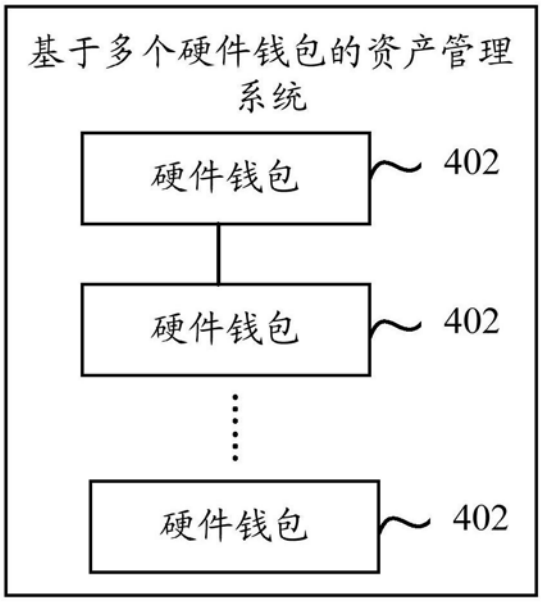

基于多个硬件钱包的资产管理系统
硬件钱包
402
硬件钱包
402
硬件钱包
402

图4

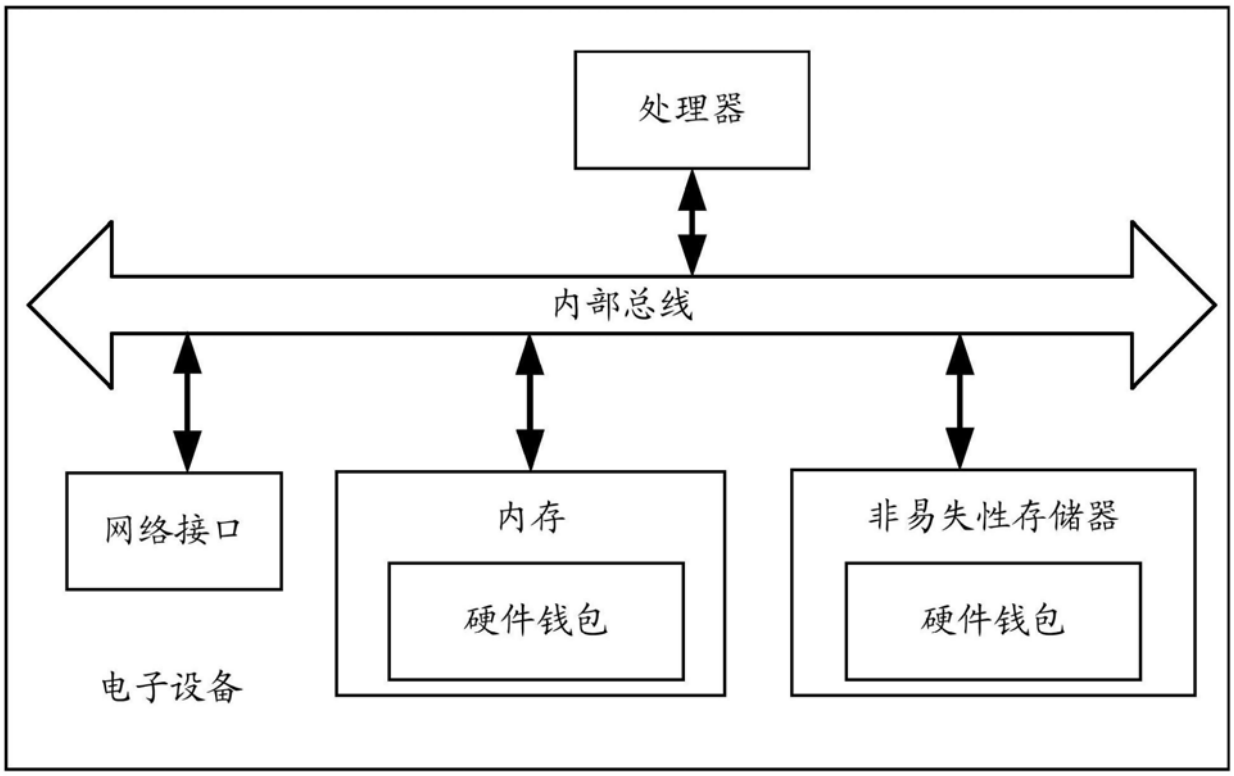

处理器
内部总线
网络接口
内存
硬件钱包
非易失性存储器
硬件钱包
电子设备

图5