



(12) 发明专利

(10) 授权公告号 CN 109389397 B

(45) 授权公告日 2021. 11. 26

(21) 申请号 201811143070.7

(22) 申请日 2018.09.28

(65) 同一申请的已公布的文献号

申请公布号 CN 109389397 A

(43) 申请公布日 2019.02.26

(73) 专利权人 北京金山安全软件有限公司

地址 100123 北京市朝阳区姚家园南路1号

惠通时代广场8号楼

(72) 发明人 雷超然 张康宗 李伟

(74) 专利代理机构 北京柏杉松知识产权代理事

务所(普通合伙) 11413

代理人 李欣 马敬

(51) Int. Cl.

G06Q 20/36 (2012.01)

(56) 对比文件

CN 101621375 A, 2010.01.06

CN 101694778 A, 2010.04.14

CN 108537537 A, 2018.09.14

CN 107920052 A, 2018.04.17

CN 106407766 A, 2017.02.15

CN 108400868 A, 2018.08.14

US 2015324787 A1, 2015.11.12

审查员 蒋健君

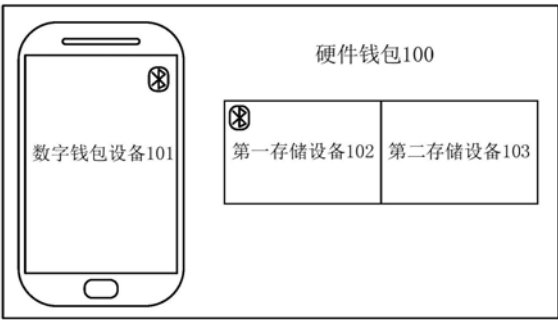
权利要求书2页 说明书7页 附图3页

(54) 发明名称

一种硬件钱包

(57) 摘要

本发明实施例提供了一种硬件钱包,包括:数字钱包设备,用于获得对目标数据进行分割所得到的第一子数据、第二子数据和第三子数据;确定数字钱包设备、第一存储设备和第二存储设备待存储的子数据;将数字钱包设备待存储的子数据存储在本地;将第一存储设备和第二存储设备待存储的子数据发送给第一存储设备;第一存储设备,用于接收数字钱包设备发送的、第一存储设备和第二存储设备待存储的子数据;保存第一存储设备待存储的子数据,将第二存储设备待存储的子数据发送给第二存储设备;第二存储设备,用于接收并保存第一存储设备发送的、第二存储设备待存储的子数据。这样,增加了私钥的盗取难度,提高了私钥的安全性,保证了数字钱包中资产的安全。



1. 一种硬件钱包, 其特征在于, 所述硬件钱包包括: 数字钱包设备、第一存储设备和第二存储设备; 所述第一存储设备插拔电连接至所述第二存储设备;

所述数字钱包设备用于: 获得对目标数据进行分割所得到的第一子数据、第二子数据和第三子数据; 其中, 所述目标数据包括: 私钥或私钥加密文件; 确定所述数字钱包设备、所述第一存储设备和所述第二存储设备待存储的子数据; 其中, 通过所述数字钱包设备、所述第一存储设备和所述第二存储设备中任意两个设备待存储的子数据能够恢复得到所述目标数据; 将所述数字钱包设备待存储的子数据存储在该数字钱包设备本地; 将所述第一存储设备和所述第二存储设备待存储的子数据发送给所述第一存储设备;

所述第一存储设备用于: 接收所述数字钱包设备发送的、所述第一存储设备和所述第二存储设备待存储的子数据; 保存所述第一存储设备待存储的子数据, 并将所述第二存储设备待存储的子数据发送给所述第二存储设备;

所述第二存储设备用于: 接收并保存所述第一存储设备发送的、所述第二存储设备待存储的子数据;

所述数字钱包设备执行的确定所述数字钱包设备、所述第一存储设备和所述第二存储设备待存储的子数据的操作包括:

确定所述数字钱包设备待存储的子数据包括: 第一子数据和第二子数据; 确定所述第一存储设备待存储的子数据包括: 第一子数据和第三子数据; 确定所述第二存储设备待存储的子数据包括: 第二子数据和第三子数据;

第一存储设备中包括: 供电模块、显示屏模块、接发模块、存储模块、闪光灯模块;

所述供电模块用于: 为所述接发模块、所述存储模块、所述闪光灯模块以及所述第二存储设备中的存储芯片供电;

所述显示屏模块用于: 显示所述供电模块的剩余电量、数字钱包设备的标识信息和数字钱包设备所执行的数字货币交易的交易金额中的至少一项。

2. 根据权利要求1所述的硬件钱包, 其特征在于, 所述第一存储设备通过通用串行总线USB接口插拔电连接至所述第二存储设备;

所述第一存储设备执行的将所述第二存储设备待存储的子数据发送给所述第二存储设备的操作包括: 通过所述USB接口将所述第二存储设备待存储的子数据发送给所述第二存储设备。

3. 根据权利要求2所述的硬件钱包, 其特征在于, 所述数字钱包设备执行的将所述第一存储设备和所述第二存储设备待存储的子数据发送给所述第一存储设备的操作包括: 通过无线通信方式, 将所述第一存储设备和所述第二存储设备待存储的子数据发送给所述第一存储设备。

4. 根据权利要求3所述的硬件钱包, 其特征在于, 所述无线通信方式包括: 蓝牙通信方式或近距离无线通信NFC通信方式。

5. 根据权利要求1所述的硬件钱包, 其特征在于, 所述数字钱包设备执行的获得对目标数据进行分割所得到的第一子数据、第二子数据和第三子数据的操作包括:

利用预设秘密共享算法对目标数据进行分割计算, 得到第一子数据、第二子数据和第三子数据。

6. 根据权利要求5所述的硬件钱包, 其特征在于, 在所述数字钱包设备利用预设秘密共

享算法对目标数据进行分割计算,得到第一子数据、第二子数据和第三子数据之前,所述数字钱包设备还用于:

利用第一预设加密算法对私钥进行加密计算,得到目标数据。

7. 根据权利要求1-6中任一项所述的硬件钱包,其特征在于,所述第一存储设备还用于:当接收到针对所述目标数据的恢复指令时,利用第二预设加密算法对所述第一存储设备所存储的子数据进行加密,得到子数据加密文件;将所述子数据加密文件发送给所述数字钱包设备;

所述数字钱包设备还用于:基于所述第二预设加密算法对所述子数据加密文件进行解密,得到所述第一存储设备所存储的子数据;利用所述第一存储设备所存储的子数据和所述数字钱包设备本地存储的子数据,恢复所述目标数据。

8. 根据权利要求1所述的硬件钱包,其特征在于,所述接发模块和所述存储模块电连接;

所述接发模块用于:接收所述数字钱包设备发送的、所述第一存储设备和所述第二存储设备待存储的子数据,将所述第二存储设备待存储的子数据发送给所述第二存储设备;

所述存储模块用于:保存所述接发模块接收到的、所述第一存储设备待存储的子数据。

9. 根据权利要求8所述的硬件钱包,其特征在于,所述接发模块、所述存储模块和所述闪光灯模块与所述供电模块电连接;

所述闪光灯模块用于:当接收到闪光灯开启指令时,启动闪光灯。

10. 根据权利要求1所述的硬件钱包,其特征在于,第一存储设备包括:第一存储盘;所述第二存储设备包括:第二存储盘。

一种硬件钱包

技术领域

[0001] 本发明涉及区块链技术领域,特别是涉及一种硬件钱包。

背景技术

[0002] 随着技术的发展,越来越多的用户使用电子设备中安装的数字钱包来管理数字货币(例如比特币和莱特币等)。其中,该电子设备也可以称为数字钱包设备。该数字钱包是基于区块链技术的钱包,且私钥是管理数字钱包中的数字货币的唯一凭证。

[0003] 发明人在实现本发明的过程中发现,数字钱包中存储有完整的私钥,该种存储方式使得完整的私钥容易被恶意用户一次性盗取。而当数字钱包中的私钥被盗取时,会造成数字货币被盗的安全隐患,无法保证用户的资产安全。

发明内容

[0004] 本发明实施例的目的在于提供一种硬件钱包,以增加恶意用户盗取私钥的难度,从而提高私钥的安全性,进而保证数字钱包中资产的安全。具体技术方案如下:

[0005] 本发明实施例提供了一种硬件钱包,该硬件钱包可以包括:数字钱包设备、第一存储设备和第二存储设备;第一存储设备插拔电连接至第二存储设备;

[0006] 数字钱包设备用于:获得对目标数据进行分割所得到的第一子数据、第二子数据和第三子数据;其中,目标数据包括:私钥或私钥加密文件;确定数字钱包设备、第一存储设备和第二存储设备待存储的子数据;其中,通过数字钱包设备、第一存储设备和第二存储设备中任意两个设备待存储的子数据能够恢复得到目标数据;将数字钱包设备待存储的子数据存储在数字钱包设备本地;将第一存储设备和第二存储设备待存储的子数据发送给第一存储设备;

[0007] 第一存储设备用于:接收数字钱包设备发送的、第一存储设备和第二存储设备待存储的子数据;保存第一存储设备待存储的子数据,并将第二存储设备待存储的子数据发送给第二存储设备;

[0008] 第二存储设备用于:接收并保存第一存储设备发送的、第二存储设备待存储的子数据。

[0009] 可选地,第一存储设备通过通用串行总线USB接口插拔电连接至第二存储设备;

[0010] 第一存储设备执行的将第二存储设备待存储的子数据发送给第二存储设备的操作包括:通过USB接口将第二存储设备待存储的子数据发送给第二存储设备。

[0011] 可选地,数字钱包设备执行的将第一存储设备和第二存储设备待存储的子数据发送给第一存储设备的操作可以包括:通过无线通信方式,将第一存储设备和第二存储设备待存储的子数据发送给第一存储设备。

[0012] 可选地,无线通信方式可以包括:蓝牙通信方式或近距离无线通信NFC通信方式。

[0013] 可选地,数字钱包设备执行的获得对目标数据进行分割所得到的第一子数据、第二子数据和第三子数据的操作可以包括:

[0014] 利用预设秘密共享算法对目标数据进行分割计算,得到第一子数据、第二子数据和第三子数据。

[0015] 可选地,在数字钱包设备利用预设秘密共享算法对目标数据进行分割计算,得到第一子数据、第二子数据和第三子数据之前,数字钱包设备还可以用于:

[0016] 利用第一预设加密算法对私钥进行加密计算,得到目标数据。

[0017] 可选地,数字钱包设备执行的确定数字钱包设备、第一存储设备和第二存储设备待存储的子数据的操作可以包括:

[0018] 确定数字钱包设备待存储的子数据包括:第一子数据和第二子数据;确定第一存储设备待存储的子数据包括:第一子数据和第三子数据;确定第二存储设备待存储的子数据包括:第二子数据和第三子数据。

[0019] 可选地,第一存储设备还可以用于:当接收到针对目标数据的恢复指令时,利用第二预设加密算法对第一存储设备所存储的子数据进行加密,得到子数据加密文件;将子数据加密文件发送给数字钱包设备;

[0020] 数字钱包设备还可以用于:基于第二预设加密算法对子数据加密文件进行解密,得到第一存储设备所存储的子数据;利用第一存储设备所存储的子数据和数字钱包设备本地存储的子数据,恢复目标数据。

[0021] 可选地,第一存储设备中包括:接发模块和存储模块;接发模块和存储模块电连接;

[0022] 接发模块用于:接收数字钱包设备发送的、第一存储设备和第二存储设备待存储的子数据,将第二存储设备待存储的子数据发送给第二存储设备;

[0023] 存储模块用于:保存接发模块接收到的、第一存储设备待存储的子数据。

[0024] 可选地,第一存储设备中还包括:供电模块和闪光灯模块;接发模块、存储模块和闪光灯模块与供电模块电连接;

[0025] 供电模块用于:为接发模块、存储模块和闪光灯模块供电;

[0026] 闪光灯模块用于:当接收到闪光灯开启指令时,启动闪光灯。

[0027] 可选地,第一存储设备中还可以包括:显示屏模块;

[0028] 显示屏模块可以用于:显示供电模块的剩余电量、数字钱包设备的标识信息和数字钱包设备所执行的数字货币交易的交易金额中的至少一项。

[0029] 可选地,第一存储设备包括:第一存储盘;第二存储设备包括:第二存储盘。

[0030] 在本发明实施例中,硬件钱包包括数字钱包设备、第一存储设备和第二存储设备。数字钱包设备可以获得第一子数据、第二子数据和第三子数据。该第一子数据、第二子数据和第三子数据是对目标数据进行分割得到的。该目标数据包括私钥或私钥加密文件。然后,该数字钱包设备可以确定数字钱包设备自身、第一存储设备和第二存储设备待存储的子数据。其中,通过数字钱包设备、第一存储设备和第二存储设备中任意两个设备待存储的子数据能够恢复得到该目标数据。之后,该数字钱包设备可以将自身待存储的子数据存储在本设备,并将第一存储设备和第二存储设备待存储的子数据发送给第一存储设备。这样,第一存储设备在接收到数字钱包设备发送的、第一存储设备和第二存储设备待存储的子数据之后,第一存储设备可以将自身待存储的子数据存储在第一存储设备本地。并将第二存储设备待存储的子数据发送给第二存储设备。第二存储设备在接收到第一存储设备发送的、第

二存储设备待存储的子数据之后,可以保存该第二存储设备待存储的子数据。这样,硬件钱包中的数字钱包设备、第一存储设备和第二存储设备可以对第一子数据、第二子数据和第三子数据进行分散存储,增加恶意用户盗取私钥的难度,从而提高了私钥的安全性,进而可以保证数字钱包中资产的安全。

附图说明

[0031] 为了更清楚地说明本发明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发明的一些实施例,对于本领域普通技术人员来讲,在不付出创造性劳动的前提下,还可以根据这些附图获得其他的附图。

[0032] 图1为本发明实施例提供的一种硬件钱包的示意图;

[0033] 图2为本发明实施例提供的硬件钱包对目标数据进行存储的一种流程图;

[0034] 图3为本发明实施例提供的硬件钱包对目标数据进行恢复的一种流程图。

具体实施方式

[0035] 下面将结合本发明实施例中的附图,对本发明实施例中的技术方案进行清楚、完整地描述,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他实施例,都属于本发明保护的范围。

[0036] 为了解决现有技术中存在的技术问题,本发明实施例提供了一种硬件钱包。

[0037] 下面结合图1和图2对本发明实施例提供的硬件钱包进行详细说明。

[0038] 参见图1,本发明实施例提供的硬件钱包100可以包括:数字钱包设备101、第一存储设备102和第二存储设备103。其中,数字钱包设备101、第一存储设备102和第二存储设备103为三个独立的设备,可以分开放置。

[0039] 其中,数字钱包设备101中安装了数字钱包(即数字钱包客户端)。另外,该数字钱包设备101可以为图1所示的智能手机,也可以为台式电脑、平板电脑和智能手表,当然并不局限于此。

[0040] 第一存储设备102为能够存储数据的设备。具体地,第一存储设备102可以为一个存储盘,即第一存储盘。同理,第二存储设备103也为能够存储数据的设备。具体地,第二存储设备103可以为另一个存储盘,即第二存储盘。

[0041] 数字钱包设备101和第一存储设备102可以通过无线通信方式进行通信连接。具体地,数字钱包设备101可以通过如图1所示的蓝牙模块与第一存储设备102进行蓝牙通信。当然,数字钱包设备101也可以通过NFC(Near Field Communication,近距离无线通信)方式与第一存储设备102进行NFC通信。当然并不局限于此。

[0042] 另外,第一存储设备102和第二存储设备103可以通过插拔电连接的方式进行连接。也就是说,可以通过插/拔的方式,建立/解除第一存储设备102和第二存储设备103之间的通信连接。具体地,第一存储设备102可以通过USB(Universal Serial Bus,通用串行总线)接口插拔电连接至第二存储设备103。这样,第一存储设备102与第二存储设备103之间可以进行串口通信。

[0043] 参见图2,在本发明实施例中,数字钱包设备101、第一存储设备102和第二存储设备103可以用于执行如下操作:

[0044] S1:数字钱包设备101获得对目标数据进行分割所得到的第一子数据、第二子数据和第三子数据;其中,目标数据包括:私钥或私钥加密文件;

[0045] 在一种实现方式中,为了提高恶意用户恢复目标数据的难度,数字钱包设备101可以利用预设秘密共享算法对目标数据进行分割计算,得到第一子数据、第二子数据和第三子数据。其中,通过秘密共享算法可以更好地设计:针对目标数据的拆分方案和恢复方案。对于该种分割方式,后续需要基于该秘密共享算法对第一子数据、第二子数据和第三子数据进行数据恢复计算,从而恢复得到目标数据。

[0046] 在另一种实现方式中,数字钱包设备100也可以将目标数据直接切割为三份,得到第一子数据、第二子数据和第三子数据,这也是合理的。对于该种切割方式,后续可以对第一子数据、第二子数据和第二子数据进行拼接,从而可以恢复得到目标数据。

[0047] 其中,当目标数据为私钥时,数字钱包设备101可以对私钥进行分割。其中,私钥是管理数字钱包中的数字货币的唯一凭证。当目标数据为私钥加密文件时,数字钱包设备101可以对私钥加密文件进行分割。

[0048] 其中,对于对私钥加密文件进行分割的方式,数字钱包设备101还可以先确定待存储的私钥。然后,利用第一预设加密算法对该私钥进行加密计算,从而得到目标数据。其中,该第一预设加密算法包括但并不局限于:RSA加密算法和DES(Data Encryption Standard, 对称加密算法)。

[0049] 该种对于对私钥加密文件进行分割的方式,使得恶意用户即使能够拿到第一子数据、第二子数据和第三子数据,并利用第一子数据、第二子数据和第三子数据恢复得到目标数据,也难以对目标数据进行解密。这样,提高了恶意用户获取私钥的难度。

[0050] 在对目标数据进行分割之后,数字钱包设备101可以获取对目标数据进行分割所得到的第一子数据、第二子数据和第三子数据。

[0051] 当然,该第一子数据、第二子数据和第三子数据也可以是除了数字钱包设备101之外的设备对目标数据进行切割后得到的。在该种方式中,数字钱包设备101可以从该设备中获取第一子数据、第二子数据和第三子数据,这也是合理的。

[0052] S2:数字钱包设备101确定数字钱包设备101、第一存储设备102和第二存储设备103待存储的子数据;其中,通过数字钱包设备101、第一存储设备102和第二存储设备103中任意两个设备待存储的子数据能够恢复得到目标数据;

[0053] 其中,通过数字钱包设备101、第一存储设备102和第二存储设备103中任意两个设备待存储的子数据能够恢复得到目标数据是指:至少需要数字钱包设备101、第一存储设备102和第二存储设备103中两个设备中待存储的子数据才能恢复得到目标数据。也就是说,通过数字钱包设备101或第一存储设备102或第二存储设备103中待存储的子数据无法恢复得到目标数据。这样,使得恶意用户在获得数字钱包设备101、第一存储设备102和第二存储设备103中的任意一个设备之后,无法对目标数据进行恢复,提高了私钥的安全性。

[0054] 示例性地,可以确定得到数字钱包设备101待存储的子数据可以包括:第一子数据和第二子数据;第一存储设备102待存储的子数据可以包括:第一子数据和第三子数据;第二存储设备103待存储的子数据包括:第二子数据和第三子数据。

[0055] 当然,也可以确定得到数字钱包设备101待存储的子数据可以包括:第一子数据和第三子数据;第一存储设备102待存储的子数据可以包括:第一子数据和第二子数据;第二存储设备103待存储的子数据包括:第二子数据和第三子数据,这也是合理的。

[0056] S3:数字钱包设备101将数字钱包设备101待存储的子数据存储于数字钱包设备101本地;

[0057] S4:数字钱包设备101发送第一存储设备102和第二存储设备103待存储的子数据至第一存储设备102;

[0058] 数字钱包设备101在确定各个设备待存储的子数据之后,可以将自身待存储的子数据存储于数字钱包设备101本地。然后,将第一存储设备102和第二存储设备103待存储的子数据均发送至第一存储设备102。

[0059] 其中,数字钱包设备101可以通过蓝牙通信方式或近距离无线通信NFC通信方式,将第一存储设备102和第二存储设备103待存储的子数据均发送至第一存储设备102,当然并不局限于此。

[0060] S5:第一存储设备102保存第一存储设备102待存储的子数据;

[0061] S6:第一存储设备102发送第二存储设备103待存储的子数据至第二存储设备103;

[0062] 第一存储设备102在接收到数字钱包设备发送的、第一存储设备102和第二存储设备103待存储的子数据之后,可以对第一存储设备102待存储的子数据进行存储,并可以将第二存储设备103待存储的数据发送至第二存储设备103。这样,可以通过第一存储设备102将数字钱包设备101所发送的、第二存储设备103待存储的子数据转发给第二存储设备103。

[0063] 其中,第一存储设备102中可以包括接发模块和存储模块。该接发模块与该存储模块电连接。其中,该接发模块可以用于:接收数字钱包设备发送的、第一存储设备102和第二存储设备103待存储的子数据,并将第二存储设备102待存储的子数据发送给第二存储设备103。该存储模块可以用于:保存接发模块接收到的、第一存储设备102待存储的子数据。

[0064] 另外,第一存储设备102中还可以包括:供电模块和闪光灯模块。其中,接发模块、存储模块和闪光灯模块与供电模块电连接。该供电模块用于为第一存储设备102中的接发模块、存储模块和闪光灯模块供电。另外,当第一存储设备102和第二存储设备103处于电连接状态时,该供电模块还用于为第二存储设备103中的存储芯片供电。

[0065] 该闪光灯模块用于当接收到闪光灯开启指令时,启动闪光灯。该闪光灯模块可以包括发光条,该发光条可以设置在第一存储设备的外部轮廓。其中,当该闪光灯模块被启动时,该发光条处于点亮状态,提高了用户的视觉体验。

[0066] 该第一存储设备102中还可以包括:显示屏模块。该显示屏模块可以用于显示供电模块的剩余电量。这样,使用户可以在显示屏上看到供电模块的电量,进而可以决定是否对第一存储设备进行充电或更换电池,从而保证第一存储设备102的正常使用。

[0067] 该显示屏模块还可以显示该数字钱包设备101的标识信息。这样,使得用户可以查看:与该第一存储设备102建立无线通信连接的数字钱包设备是否为用户想要连接的数字钱包设备101。当不是用户想要连接的数字钱包设备时,用户可以及时将想要连接的数字钱包设备101与该第一存储设备102进行通信连接。其中,该数字钱包设备101的标识信息包括但不限于:用户给该数字钱包设备101设置的自定义名称、该数字钱包设备101的产品序列号和该数字钱包设备101的MAC(Media Access Control,媒体访问控制)地址。

[0068] 该显示屏模块还可以显示该数字钱包设备101所执行的数字货币交易的交易金额。这样,使得用户可以通过第一存储设备101中显示屏查看到数字货币交易的交易金额,便于用户确认交易金额是否正确。

[0069] S7:第二存储设备103保存第一存储设备发送的、第二存储设备102待存储的子数据。

[0070] 其中,当第二存储设备103存储了其待存储的子数据之后,则可以实现将私钥或私钥加密文件所分割得到的第一子数据、第二子数据和第三子数据分散存储至数字钱包设备101、第一存储设备102和第二存储设备103中,即实现了对私钥的分散存储。这样,使得通过数字钱包设备101、第一存储设备102和第二存储设备103中的任一设备均不能对目标数据进行恢复,增加了恶意用户盗取私钥的难度,从而提高私钥的安全性,进而保证数字钱包中资产的安全。

[0071] 在本发明实施例中,硬件钱包包括数字钱包设备、第一存储设备和第二存储设备。数字钱包设备可以获得第一子数据、第二子数据和第三子数据。该第一子数据、第二子数据和第三子数据是对目标数据进行分割得到的。该目标数据包括私钥或私钥加密文件。然后,该数字钱包设备可以确定数字钱包设备自身、第一存储设备和第二存储设备待存储的子数据。其中,通过数字钱包设备、第一存储设备和第二存储设备中任意两个设备待存储的子数据能够恢复得到该目标数据。之后,该数字钱包设备可以将自身待存储的子数据存储在本地,并将第一存储设备和第二存储设备待存储的子数据发送给第一存储设备。这样,第一存储设备在接收到数字钱包设备发送的、第一存储设备和第二存储设备待存储的子数据之后,第一存储设备可以将自身待存储的子数据存储在第一存储设备本地。并将第二存储设备待存储的子数据发送给第二存储设备。第二存储设备在接收到第一存储设备发送的、第二存储设备待存储的子数据之后,可以保存该第二存储设备待存储的子数据。这样,硬件钱包中的数字钱包设备、第一存储设备和第二存储设备可以对第一子数据、第二子数据和第三子数据进行分散存储,增加恶意用户盗取私钥的难度,从而提高了私钥的安全性,进而可以保证数字钱包中资产的安全。

[0072] 在本发明实施例提供的硬件钱包完成对私钥的分散存储之后,当数字钱包设备101接收到用户触发的目标数据恢复指令时(例如用户点击数字钱包中弹出的确认支付按钮),参见图3,数字钱包设备101、第一存储设备102和第二存储设备103还可以执行如下操作:

[0073] S8:数字钱包设备101向第一存储设备102发送针对目标数据的恢复指令;

[0074] S9:第一存储设备102利用第二预设加密算法,对第一存储设备102所存储的子数据进行加密,得到子数据加密文件;

[0075] 该第二预设加密算法包括但并不局限于:RSA加密算法和DES(Data Encryption Standard,对称加密算法)。

[0076] S10:第一存储设备102向数字钱包设备101发送该子数据加密文件;

[0077] 其中,通过对第一存储设备102所存储的子数据进行加密,并对加密得到的子数据加密文件进行传输。这样,可以避免第一存储设备102所存储的子数据在传输过程中被恶意用户截取,保证了第一存储设备102所存储的子数据的安全,从而进一步保证了私钥的安全。

[0078] S11:数字钱包设备101基于第二预设加密算法对该子数据加密文件进行解密,得到第一存储设备102所存储的子数据;

[0079] S12:数字钱包设备101利用第一存储设备所存储的子数据和数字钱包设备本地存储的子数据,恢复目标数据。

[0080] 假设第一存储设备102中所存储的子数据为第一子数据和第三子数据,数字钱包设备101中所存储的子数据为第一子数据和第二子数据。那么,当第一子数据、第二子数据和第三子数据是利用预设秘密共享算法对目标数据进行分割计算所得到的时,可以基于该秘密共享算法对第一子数据、第二子数据和第三子数据进行数据恢复计算,从而恢复得到目标数据。

[0081] 当第一子数据、第二子数据和第三子数据是对目标数据进行直接切割所得到的数据时,可以对第一子数据、第二子数据和第二子数据进行拼接,从而可以恢复得到目标数据。

[0082] 以上,可以在通过硬件钱包对私钥或私钥加密数据进行分散存储之后,当数字钱包设备101在接收到针对目标数据的恢复指令时,可以从第一存储设备102中获得子数据。然后,可以利用数字钱包设备101本地存储的子数据和从第一存储设备102中获得子数据来恢复目标数据,进而恢复得到私钥。

[0083] 综上,应用本发明实施例提供的硬件钱包,可以对私钥或私钥加密数据进行分散存储,增加了恶意用户盗取私钥的难度,从而提高了私钥的安全性,进而可以保证数字钱包中资产的安全。另外,本发明实施例提供的硬件钱包还可以对私钥进行恢复,保证数字钱包的正常使用。

[0084] 需要说明的是,在本文中,诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来,而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且,术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含,从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素,而且还包括没有明确列出的其他要素,或者是还包括为这种过程、方法、物品或者设备所固有的要素。在没有更多限制的情况下,由语句“包括一个……”限定的要素,并不排除在包括所述要素的过程、方法、物品或者设备中还存在另外的相同要素。

[0085] 本说明书中的各个实施例均采用相关的方式描述,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。

[0086] 以上所述仅为本发明的较佳实施例而已,并非用于限定本发明的保护范围。凡在本发明的精神和原则之内所作的任何修改、等同替换、改进等,均包含在本发明的保护范围内。

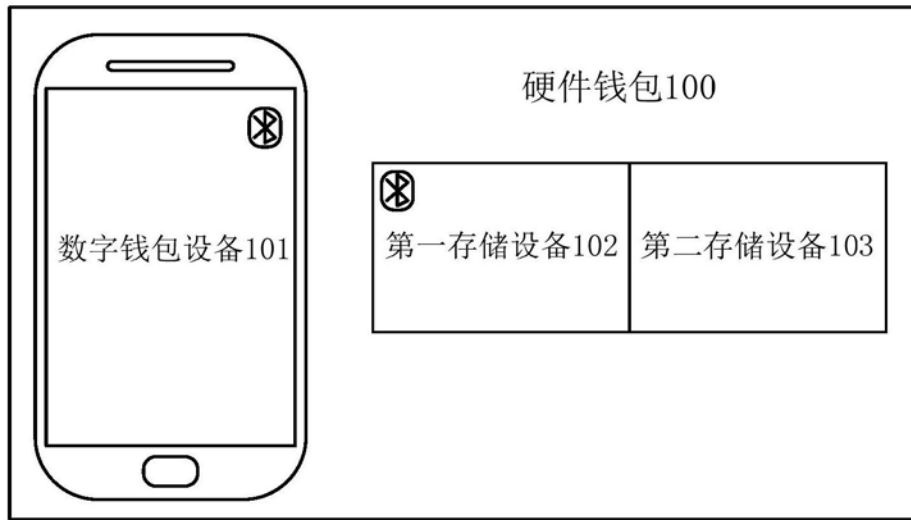


图1

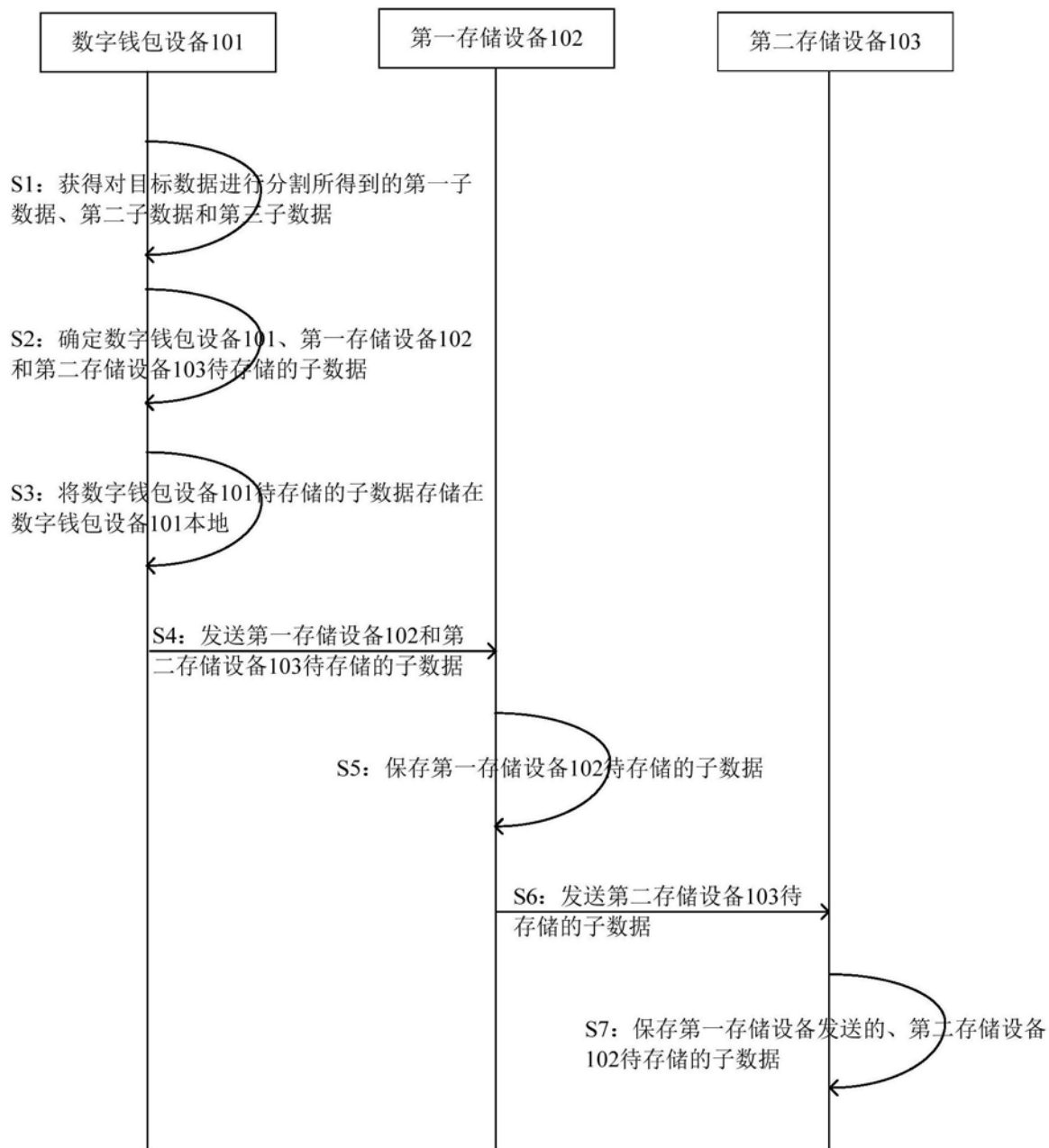


图2

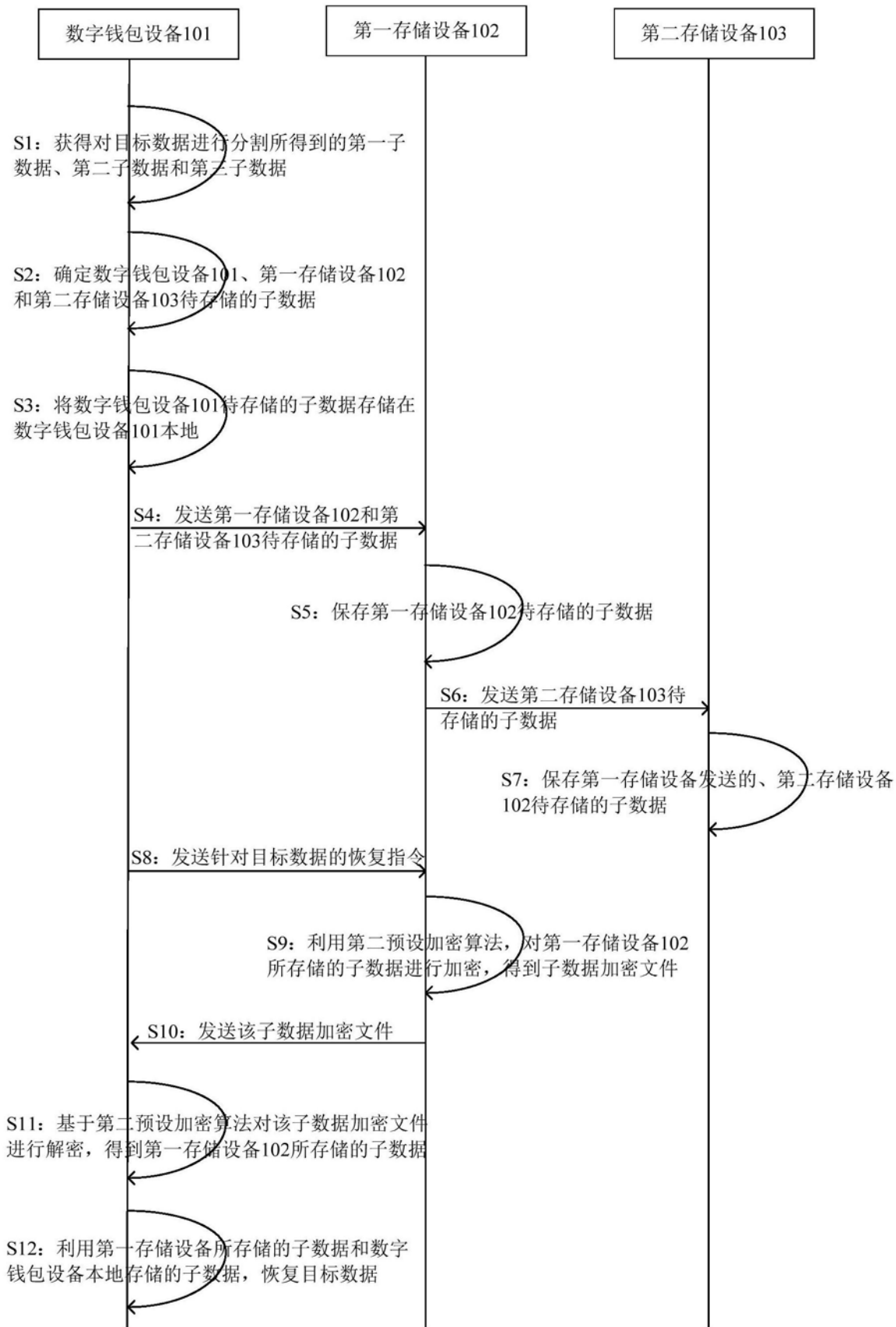


图3