(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 112352238 A
(43)申请公布日 2021.02.09

(21)申请号 201980042693.1

(22)申请日 2019.06.28

(30)优先权数据
10-2018-0075039 2018.06.28 KR

(85)PCT国际申请进入国家阶段日
2020.12.24

(86)PCT国际申请的申请数据
PCT/KR2019/007927 2019.06.28

(87)PCT国际申请的公布数据
WO2020/005034 KO 2020.01.02

(71)申请人 币即特株式会社
地址 韩国首尔市

(72)发明人 李东山

(74)专利代理机构 北京铭硕知识产权代理有限公司 11286
代理人 习瑞恒 李盛泉

(51)Int.Cl.
G06F 21/33(2006.01)
H04L 9/32(2006.01)

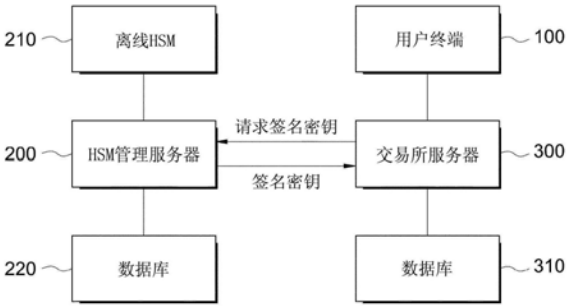
权利要求书1页 说明书7页 附图3页

(54)发明名称

多重签名安全帐户控制系统

(57)摘要

本发明涉及一种多重签名安全帐户控制系统。本发明可以包括至少三个参与账户具有管理权限的多重签名安全账户,其中,所述参与账户包括与用户终端相应的第一参与账户、与硬件安全模块管理服务器相应的第二参与账户、与交易所服务器相应的第三参与账户,在硬件安全模块管理服务器中进行控制以使用由至少两个参与账户提供的签名信息而对所述多重签名安全账户的权限进行管控。



CN 112352238 A

1.一种多重签名安全帐户控制系统,其特征在于,

包括至少三个参与账户具有管理权限的多重签名安全账户,其中,所述参与账户包括与用户终端(100)相应的第一参与账户、与硬件安全模块管理服务器(200)相应的第二参与账户、与交易所服务器(300)相应的第三参与账户,

在硬件安全模块管理服务器(200)中进行控制以使用由预先设定的数量以上的参与账户提供的签名信息而对所述多重签名安全账户的权限进行管控。

2.根据权利要求1所述的多重签名安全帐户控制系统,其特征在于,

所述多重签名安全账户的权限为资产的转移、对资产转移及设定变更的权限委任/委任撤销、生产者投票、余额确认、交易目录显示、投标价格信息获取、物品的购买及销售、许可控制、提案书的提案/实行、提案书审核/批准/拒绝中的至少一个权限。

3.根据权利要求1所述的多重签名安全帐户控制系统,其特征在于,

所述多重签名安全账户的各参与主体持有所有权,并且通过所述参与主体所持有的权重确定多重签名安全账户的份额。

4.根据权利要求1所述的多重签名安全帐户控制系统,其特征在于,

所述多重签名安全账户构成为,在多个参与账户中的一个发生侵害的情况下,通过其余参与账户的认证而将被侵害的账户的权限变更为新的参与账户。

5.根据权利要求1所述的多重签名安全帐户控制系统,其特征在于,包括:

离线硬件安全模块(210),针对至少三个参与账户具有管理权限的多重签名安全账户中的第二参与账户,在线下生成私钥和公钥;

所述硬件安全模块管理服务器(200),接收在所述离线硬件安全模块(210)生成的私钥和公钥,并将所述私钥存储于数据库(220),生成密钥加密密钥和数据密钥,并且通过密钥加密密钥将所述数据密钥加密并存储于数据库(220),并输出通过所述数据密钥加密的签名信息;

数据库(220),存储所述私钥、密钥加密密钥、数据密钥,

其中,所述硬件安全模块管理服务器(200)进行控制来构成第二参与账户、用户终端(100)的第一参与账户和交易所服务器(300)的第三参与账户具有管理权限的多重签名安全账户,从而通过多重签名信息的认证,来管控所述多重签名安全账户的权限。

6.根据权利要求5所述的多重签名安全帐户控制系统,其特征在于,

所述硬件安全模块管理服务器(200)进行控制使得在第一参与账户和第三参与账户中的一个账户被侵害(或被黑客攻击)的情况下,通过预先设定的验证过程,被侵害的账户的权限变更为新的账户。

多重签名安全帐户控制系统

技术领域

[0001] 本发明涉及一种多重签名安全帐户控制系统,尤其涉及一种如下的多重签名安全帐户控制系统:通过多个账户签名控制对账户的管理权限,从而如果对任意账户具有管理权限的至少三个参与账户中的预先设定的数量以上的参与账户进行签名,则能够行使对任意账户的管理权限,以保持账户的安全,从而管理账户的控制及恢复。

背景技术

[0002] 加密货币是通过以信息形态存留于计算机等且没有实物而只能在互联网上进行交易的一种电子货币。

[0003] 初期,加密货币作为肉眼不可见并表现在计算机上的货币,因此被称为数字货币(Digital currency)或虚拟货币等,但最近也被称为加密货币,以表示其为使用加密技术的货币的含义。

[0004] 加密货币不会产生由于货币发行引起的生产费用,从而可以大幅减少转账费用等交易费用,并且由于是没有实物而仅在网络上进行交易的网络型电子货币,因此对持有数量没有限制。

[0005] 并且,由于无需经过中间步骤,因此具有能够立即进行交易的优点。

[0006] 这种加密货币代表性地包括“比特币”、“以太坊币”、“EOS币”、“莱特币”、“新经币”、“门罗币”、“达世币”。等。

[0007] 这种加密货币在区块链(Block chain)系统中驱动,区块链技术为用于记录加密货币交易明细的分散型账簿记录数据库技术。

[0008] 所有加密货币的用户端均由作为私钥和公钥(地址)形式的一对密钥构成。

[0009] 例如,公钥对应于银行的账号,私钥对应于密码,公钥和私钥由仅在彼此之间相互匹配的一对构成。

[0010] 通常,对于加密货币QT程序(用户个人钱包程序)而言,利用用户密码对私钥进行加密而存储于会员计算机等的用户终端。

[0011] 对于加密货币交易所而言,利用用户密码或服务器的盐(SALT)对私钥进行加密而存储于交易所服务器。

[0012] 但是,存储用户信息的现有的构成具有存在如下可能性的问题,即,通过知道加密方式的交易所安全相关内部人员或黑客攻击等,对存储于交易所服务器的相应加密的私钥进行解密,并从用户的账户非法转移资产。

[0013] 即,存在着如下的问题:若构成为能够利用一个密码来管控资产的移动与否和针对账户的权限并且发生黑客攻击等,则可能无法使用账户。

[0014] 并且,即使在用户持有钱包的情况下,由于本人不具有本人的账户的管理权限,而是依赖于交易所,因此如果发生针对交易所的黑客攻击,则可能无可奈何地承担损失。

[0015] 并且,在用户遗失私钥或者私钥被损坏的情况下,无法行使对账户的管理权限,也无法恢复,因此存在贵重的资产可能全部丢失的问题。

发明内容

[0016] 技术问题

[0017] 为了解决这样的技术问题,本方面的目的在于提供一种如下的多重签名安全帐户控制系统:通过多个账户签名控制对账户的管理权限,从而当对任意账户具有管理权限的三个以上在彼此不同的账户中设定的数量以上的参与账户进行签名时能够行使对任意账户的管理权限,以保持账户的安全,从而管理账户的控制及恢复。

[0018] 若在对任意账户具有管理权限的三个以上的参与账户中预先设定的数量以上的参与账户进行签名,则可以行使对任意账户的管理权限,因此,可以通过多个账户签名控制对账户的管理权限而管理账户的控制及恢复,因此可以提高账户的安全性

[0019] 技术方案

[0020] 为了达成上述目的,本发明的一实施例为多重签名安全帐户控制系统,其特征在于,包括至少三个参与账户具有管理权限的多重签名安全账户,其中,所述参与账户包括与用户终端相应的第一参与账户、与HSM管理服务器相应的第二参与账户、与交易所服务器相应的第三参与账户。

[0021] 并且,在根据本发明的一实施例的多重签名安全帐户控制系统中,在HSM管理服务器中进行控制以使用由预先设定的数量以上的参与账户提供的签名信息而对多重签名安全账户的权限进行管控。

[0022] 并且,根据本发明的一实施例的所述多重签名安全账户的权限为资产的转移、对资产转移及设定变更的权限委任/委任撤销、生产者投票、余额确认、交易目录显示、投标价格信息获取、物品的购买及销售、许可控制、提案书的提案/实行、提案书审核/批准/拒绝中的至少一个权限。

[0023] 并且,根据本发明的一实施例的所述多重签名安全账户的各参与主体持有所有权,并且通过所述参与主体所持有的权重确定多重签名安全账户的份额。

[0024] 并且,根据本发明的一实施例的所述多重签名安全账户构成为,在多个参与账户中的一个发生侵害的情况下,通过其余参与账户的认证而将被侵害的账户的权限变更为新的参与账户。

[0025] 并且,根据本发明的一实施例的多重签名安全帐户系统包括:离线HSM(Hardware Security Module),针对至少三个参与账户具有管理权限的多重签名安全账户中的第二参与账户,在线下生成私钥(private key)和公钥(Public key)。

[0026] 并且,根据本发明的一实施例的多重签名安全帐户系统包括:HSM管理服务器,接收在所述离线HSM生成的私钥和公钥,并将所述私钥存储于数据库,生成密钥加密密钥(KeK:Key Encryption Key)和数据密钥(DK:Data Key),并且通过密钥加密密钥(KeK:Key Encryption Key)将所述数据密钥加密并存储于数据库。

[0027] 并且,所述HSM管理服务器向用户终端或交易所服务器输出通过数据密钥加密的签名信息。

[0028] 并且,根据本发明的一实施例的多重签名安全帐户系统包括:数据库,加密的私钥、KeK、数据密钥(DK)。

[0029] 并且,根据本发明的一实施例的HSM管理服务器进行控制来构成第二参与账户、用户终端100的第一参与账户和交易所服务器的第三参与账户具有管理权限的多重签名安全

账户,从而通过多重签名(Signature)信息的认证,来管控所述多重签名安全账户的权限。

[0030] 并且,根据本发明的一实施例的HSM管理服务器进行控制使得在第一参与账户和第三参与账户中的一个账户被侵害(或黑客攻击)的情况下,通过预先设定的验证过程,被侵害的账户的权限变更为新的账户。

[0031] 有益效果

[0032] 根据本发明,若在对任意账户具有管理权限的三个以上的参与账户中预先设定的数量以上的参与账户进行签名,则可以行使对任意账户的管理权限,因此,可以通过多个账户签名控制对账户的管理权限而管理账户的控制及恢复,因此可以提高账户的安全性。

[0033] 并且,根据本发明,即使因黑客攻击等而导致账户中的一部分信息泄露,也能够通过多重签名来执行安全账户的恢复,从而具有可用于多种加密货币的交易的优点。

附图说明

[0034] 图1是示出根据本发明的一实施例的多重签名安全账户控制系统的构成的框图。

[0035] 图2是示出根据本发明的一实施例的多重签名安全账户控制系统的操作过程的流程图。

[0036] 图3是示出根据本发明的一实施例的多重签名安全账户控制系统的操作过程的另一流程图。

[0037] 图4是示出根据本发明的一实施例的多重签名安全账户控制系统的账户恢复过程的流程图。

[0038] 附图标记说明

[0039] 100:用户终端 200:HSM管理服务器

[0040] 210:离线HSM 220:数据库

[0041] 300:交易所服务器 310:数据库

具体实施方式

[0042] 图1是示出根据本发明的一实施例的多重签名安全账户控制系统的构成的框图,图2是示出根据本发明的一实施例的多重签名安全账户控制系统的操作过程的流程图,图3是示出根据本发明的一实施例的多重签名安全账户控制系统的操作过程的另一流程图,图4是示出根据本发明的一实施例的多重签名安全账户控制系统的账户恢复过程的流程图。

[0043] 如图1至图4所示,根据本发明的一实施例的多重签名安全账户控制系统包括至少三个参与账户具有管理权限的多重签名安全账户、具有各自的参与账户的用户终端100、HSM管理服务器200、交易所服务器300。

[0044] 在此,账户可以表示交易加密货币时使用的钱包。因此,用户终端100、HSM管理服务器200和交易所服务器300的参与账户也具有用于交易加密货币的各自的钱包,将该钱包称为参与账户。将使该各自的参与账户对一个任意账户具有管理权限的用于加密货币交易的账户称为多重签名安全账户。

[0045] 在此,多重签名安全账户表示包含为了账户的安全而应用了多重签名(mutisignature)技术事项这一概念的术语。账户的安全可以包括保护账户的变动事项不会由未经授权的人的行为实现的所有过程。

[0046] 多重签名表示使用多个签名而非一个签名。即,将签名的主体为多个而非一个的情况作为前提。据此,多重签名表示为了任意的认证而由多个主体分别进行签名。因此,签名的主体分别具有对任意账户的管理权限。

[0047] 因此,用户终端100、HSM管理服务器200和交易所服务器300中的每一个可以成为签名的主体,并且对任意账户行使管理权限。

[0048] 由于用户终端100、HSM管理服务器200和交易所服务器300参与对任意账户的管理权限的行使,因此被称为可以行使管理权限的参与账户。

[0049] 各个参与账户能够对任意账户行使管理权限的份额或加权值可以通过相互协商根据需要适当地确定。

[0050] 并且,在行使相应账户的管理权限时设定基准值,当存在来自各参与账户的超过该基准值的签名时,可以行使对相应账户的管理权限。

[0051] 并且,多重签名安全账户控制系统控制在HSM管理服务器200中进行控制以使用由至少两个参与账户提供的多重签名(Signature)信息(签名密钥),从而管控多重签名安全账户的权限。

[0052] 所述多重签名安全账户的权限包括资产的转移、对资产转移及设定变更的权限委任/委任撤销、生产者投票、余额确认、交易目录显示、投标价格信息获取、物品的购买及销售、许可控制、提案书的提案/实行、提案书审核/批准/拒绝中的至少一个权限。

[0053] 所述用户终端100通过网络而与交易所服务器300连接,并管理对多重签名安全账户具有管理权限的第一参与账户。

[0054] 并且,所述用户终端100可以利用台式PC、笔记本PC、平板PC、掌上计算机(palmtops)、个人数字助理(PDA:Personal Digital Assistants)、能够连接互联网的诸如智能电话的通信终端装置、便携式多媒体播放器(PMP)或超移动计算机(UMPC:Ultra-mobile PC)及移动互联网设备(MID:Mobile Internet Device)等多种终端构成。

[0055] 并且,所述用户终端100可以通过第一参与账户请求多重签名安全账户中保管的资产的移动、对资产转移及设定变更的权限委任/委任撤销、生产者投票、余额确认、交易目录显示、投标价格信息获取、物品的购买及销售、许可控制、提案书的提案/实行、提案书审核/批准/拒绝等作业。

[0056] 并且,在第一参与账户被侵害(或黑客攻击)的情况下,所述用户终端100向HSM管理服务器200请求将权限变更为根据侵害发生的新的第一参与账户。

[0057] 所述硬件安全模块(HSM:Hardware Security Module)管理服务器200生成对至少三个参与账户(在此,所述参与账户为从用户终端100生成的第一参与账户、与HSM管理服务器200相应的第二参与账户、与交易所服务器300相应的第三参与账户)具有管理权限的多重签名安全账户并进行管理。

[0058] 即,多重签名安全账户例如为,多个参与账户具有管理权限以便对利用公钥生成的账户管理针对资产的增减的账户,并且是可以根据参与账户的份额来划分所有权而构成的账户。

[0059] 并且,所述多重签名安全账户可以用于企业的金融账户的管控、团体/NGO等的金融账户的管控、P2P资金保护、买卖保护交易、区块链的使用管控等。

[0060] 并且,所述多重签名安全账户的各参与主体(即,第一参与账户、第二参与账户、第

三参与账户)持有所有权,并且通过所述第一参与账户、第二参与账户、第三参与账户的参与主体所持有的资产等的权重(Weight),可以确定多重签名安全账户的份额。

[0061] 并且,所述多重签名安全账户可以通过保险得到保护。

[0062] 所述HSM管理服务器200包括离线硬件安全模块(HSM:Hardware Security Module)210和数据库220。

[0063] 所述离线HSM 210针对由相互不同的用户生成的至少三个参与账户构成的多重签名安全账户,在线下生成私钥(private key)和公钥(Public key)。

[0064] 在所述离线HSM 210生成的私钥被加密并存储在HSM管理服务器200的数据库220或外部的数据库,从而不会泄漏到外部而能够被安全地保护并管理。

[0065] 所述HSM管理服务器200通过USB存储器等独立的存储装置接收从所述离线HSM 210生成的私钥和公钥,所述私钥被加密而存储于数据库220,公钥在所述HSM管理服务器200被公开而生成为由至少三个参与账户构成的多重签名安全账户。

[0066] 并且,HSM管理服务器200可以管理进行认证加密密钥管理解决方案、云计算、联网、支付、安全及存储。

[0067] 并且,所述HSM管理服务器200生成密钥加密密钥(KeK:Key Encryption Key)和数据密钥(DK:Data Key),并且所述数据密钥通过密钥加密密钥(KeK:Key Encryption Key)被加密并存储于数据库220。

[0068] 并且,所述HSM管理服务器200利用数据密钥(DK:Data Key)对包括签名信息的数据进行加密而生成签名密钥。

[0069] 并且,所述HSM管理服务器200将所述签名密钥提供给构成多重签名安全账户的账户,例如,第一参与账户、第二参与账户及第三参与账户,从而将其用于资产转移或权限变更的批准等,以防止存储于HSM管理服务器200的私钥泄露到外部。

[0070] 并且,所述HSM管理服务器200可以基于HSM而使KeK在HSM内部能够得到保护,并且使得KeK在离线HSM 210中保护。

[0071] 并且,所述数据密钥可以在HSM的易失性存储器中生成,并且用于私钥的加密。

[0072] 并且,所述数据密钥利用KeK公钥被加密后,为了在紧急时恢复密钥而存储于数据库220,而且未加密的数据密钥只存在于HSM的存储器。

[0073] 并且,所述HSM管理服务器200以使至少三个互不相同的账户(即,HSM管理服务器200的第二参与账户、用户终端100的第一参与账户和交易所服务器300的第三参与账户)具有管理权限的方式构成多重签名安全账户。

[0074] 并且,所述HSM管理服务器200在第一参与账户、第二参与账户、第三参与账户之间执行保密等协议和注册过程,并且执行管理员的API使用、共享秘密密钥的交换、按各个账户的用户的全局唯一识别号(GUID:Global Uniqie ID)的分配。

[0075] 并且,所述HSM管理服务器200向按各个用户的GUID追加用户信息,并使映射到所述按各个用户的GUID的密钥可以在应用了HSM或与此类似的安全系统的应用程序中得到保护。

[0076] 并且,所述HSM管理服务器200通过对三个账户中的两个以上的账户的多重签名(Multi Signature)信息(即,签名密钥)的认证进行控制,从而管控多重签名安全账户的权限。

[0077] 在多重签名安全账户中,通过利用划分至第一参与账户、第二参与账户及第三参与账户的份额和各账户的份额合计,使得由小于预先设定的临界值的份额合计构成的权限无法从多重签名安全账户转移资产或变更设定于多重签名安全账户的权限。

[0078] 即,对于多重签名安全账户,在用于批准资产转移的临界值(份额之和)例如为“50”,而第一参与账户的份额为“40”,第三参与账户的份额为“30”,第二参与账户的份额为“30”的情况下,为了从多重签名安全账户转移资产,由两个以上的账户提供签名密钥,若此时份额之和超过“50”,则可以执行对所述资产转移的批准和转移。

[0079] 另外,在本实施例中,虽然为了便于说明而以三个参与账户的情形为实施例进行了说明,但并不局限于此,根据需要,也可以由三个以上的参与账户构成,例如,在由五个参与账户构成的情况下,需要从三个以上的参与账户输入签名信息。

[0080] 并且,所述HSM管理服务器200在发生由受到侵害或黑客攻击等引起的问题时,使得能够通过多重签名恢复多重签名安全账户。

[0081] 即,所述HSM管理服务器200将第一参与账户+第三参与账户用于一般业务,将第一参与账户+第二参与账户在第三参与账户受到侵害(或黑客攻击)的情况下使用,并将第三参与账户+第二参与账户在第一参与账户受到侵害(或黑客攻击)的情况下使用两个多重签名。

[0082] 并且,所述HSM管理服务器200在第一参与账户或第三参与账户中的一个账户受到侵害(或黑客攻击)的情况下,使用两个多重签名,从而通过预先设定的验证过程,使权限从被侵害的账户变更为新的账户。

[0083] 另外,在多重签名安全账户中第一参与账户被侵害的情况下,单一账户无法移动资产或令牌,可通过第三参与账户或第二参与账户请求第一参与账户的恢复索赔。

[0084] 此时,所述HSM管理服务器200可以在进行用户识别之后,通过经用户认证的意向表示确认来允许变更为新的第一参与账户以及将权限恢复至所述新账户。

[0085] 所述用户识别过程可以包括利用预先设定的用户的护照、银行账户信息等的识别,并且还可以包括关于国际金融交易限制对象和主要政治人物信息。

[0086] 并且,针对第一参与账户,所述HSM管理服务器200可以不管理用户密码等,而是通过会话认证、利用SMS-MO/OTP/ARS的认证、用户识别(KYC)账户认证等来执行用户认证,也可以根据风险级别应用其他认证手段。

[0087] 并且,针对第三参与账户,所述HSM管理服务器200可以通过共享安全密钥认证、SMS-MO/ARS/Soft-OTP等执行认证。

[0088] 并且,所述HSM管理服务器200可以利用汇款人账号和一次性金额来执行验证,并且将为了向用户进行验证而汇款的金额(例如,1韩元)再次向管理员指定的虚拟账户汇款,从而也可以确认是否同意将权限变更为新账户。

[0089] 并且,这样的构成可以适合于应用内部管制的企业。

[0090] 所述数据库220加密并存储私钥、KeK、数据密钥(DK)等。

[0091] 所述交易所服务器300是通过网络与用户终端100、HSM管理服务器200连接并管理多重签名安全账户的第三参与账户的构成,可以利用台式计算机、笔记本计算机、服务器系统等多种终端构成,并且可以包括数据库310。

[0092] 并且,所述交易所服务器300是进行多个用户之间的关于加密货币的交易而在用

户的账户之间移动加密货币的构成。

[0093] 即,针对由用户终端100请求的从多重签名安全账户的资产移动,所述交易所服务器300可以从HSM管理服务器200接收多重签名信息而实现资产移动。

[0094] 并且,所述交易所服务器300可以通过第三参与账户请求多重签名安全账户中保管的资产的转移、对资产转移及设定变更的权限委任/委任撤销、生产者投票、余额确认、交易目录显示、投标价格信息获取、物品的购买及销售、许可控制、提案书的提案/实行、提案书审核/批准/拒绝等作业。

[0095] 并且,所述交易所服务器300在第三参与账户受到侵害(或黑客攻击)的情况下,可以向HSM管理服务器200请求将权限变更为根据侵害发生的新的第三参与账户。

[0096] 接下来,对多重签名安全账户的使用过程进行说明。

[0097] 首先,若用户终端100向HSM管理服务器200执行会员加入(S100),则交易所服务器300执行利用由所述HSM管理服务器200发送的用户信息(S110)的用户信息认证(S120),进而按各个用户分配GUID(S130)并发送至HSM管理服务器200及用户终端100(S140)。

[0098] 即,在第一参与账户、第二参与账户、第三参与账户之间执行保密等合同及注册、管理员的API使用、共享密钥的交换、按各个用户的GUID的分配之后,添加用户信息。

[0099] 此时,也可以验证包括AML检查的用户信息。

[0100] 生成的所述按各个用户的GUID在HSM管理服务器200的HSM受到保护,并且将签名密钥映射到多签名安全账户。

[0101] 之后,若从用户终端100输入关于资产转移的请求(S200),则HSM管理服务器200生成关于多重签名安全账户的多重签名(S210),若向用户终端100确认了多重签名(S220)和多重签名批准(S230),则执行资产转账(S240)。

[0102] 另外,若多重签名安全账户的第一参与账户发生侵害而从用户终端100输入账户恢复请求(S300),则HSM管理服务器200生成多重签名(S310),从而在用户识别之后,通过经用户认证的意向显示确认来行使变更为新的第一参与账户和恢复为所述新账户的权限。

[0103] 生成的所述多重签名传送至交易所服务器300而执行确认过程(S320)。

[0104] 若在交易所服务器300确认批准(S330),则HSM管理服务器200批准包括新的第一参与账户的多重签名安全账户的恢复(S340),并将结果传送至用户终端100(S350)。

[0105] 因此,对于由三个以上的互不相同的账户构成的多重签名安全账户,通过多个账户签名管理安全账户的控制及恢复,从而可以提高安全性。

[0106] 如上所述,参照本发明的优选实施例进行了说明,但是只要是本技术领域的熟练的技术人员,就可以理解在不脱离权利要求书中记载的本发明的思想及领域的范围内可以对本发明进行多种修改及变更。

[0107] 另外,在本发明的权利要求书中记载的附图标记只是为了说明的明确性和便利而记载,并非限定于此,在对实施例进行说明的过程中,附图中图示的线的厚度或构成要素的大小等可能为了说明的明确性和便利而夸张地进行图示,上述的术语是考虑在本发明中的功能而定义的术语,其可能会根据使用者、运用者的意图或惯例而不同,因此,对这些术语的解释应以本说明书通篇内容为基础进行。

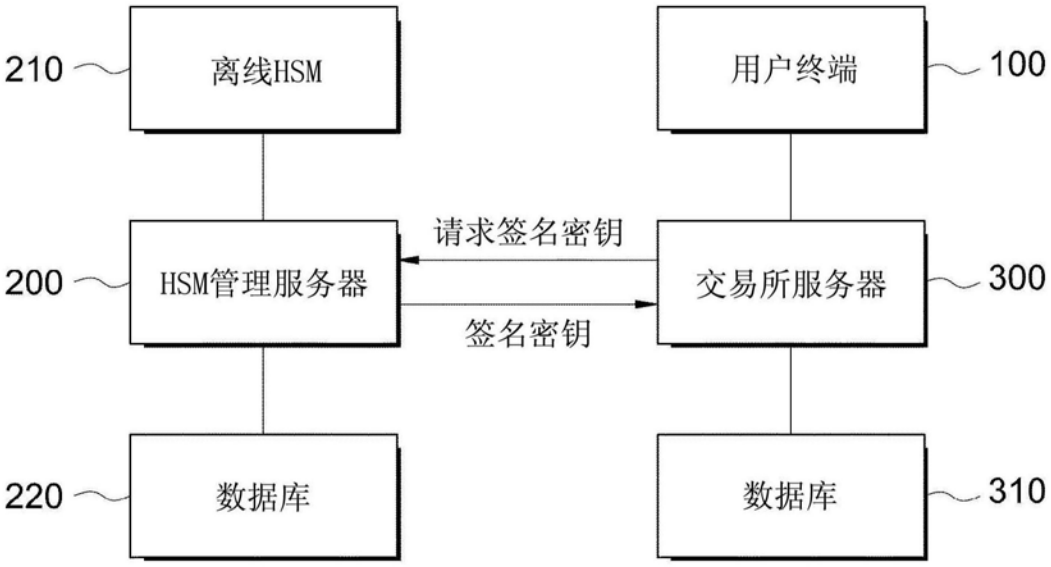

210
离线HSM
用户终端
100
请求签名密钥
200
HSM管理服务器
交易所服务器
300
签名密钥
220
数据库
数据库
310

图1

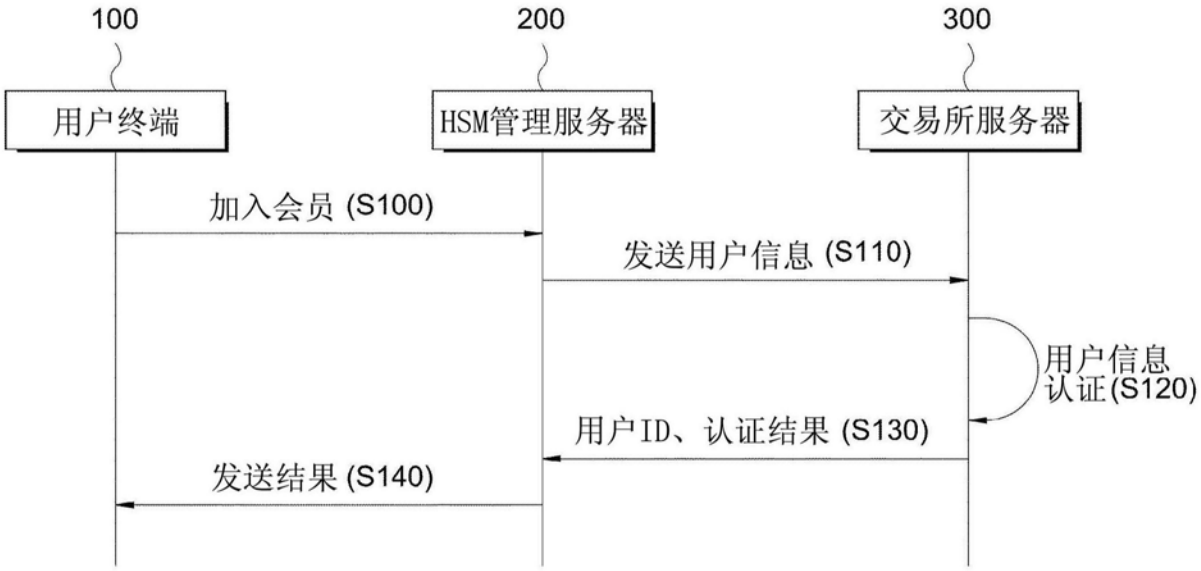

100
200
300
用户终端
HSM管理服务器
交易所服务器
加入会员 (S100)
发送用户信息 (S110)
用户信息
认证(S120)
用户ID、认证结果 (S130)
发送结果 (S140)

图2

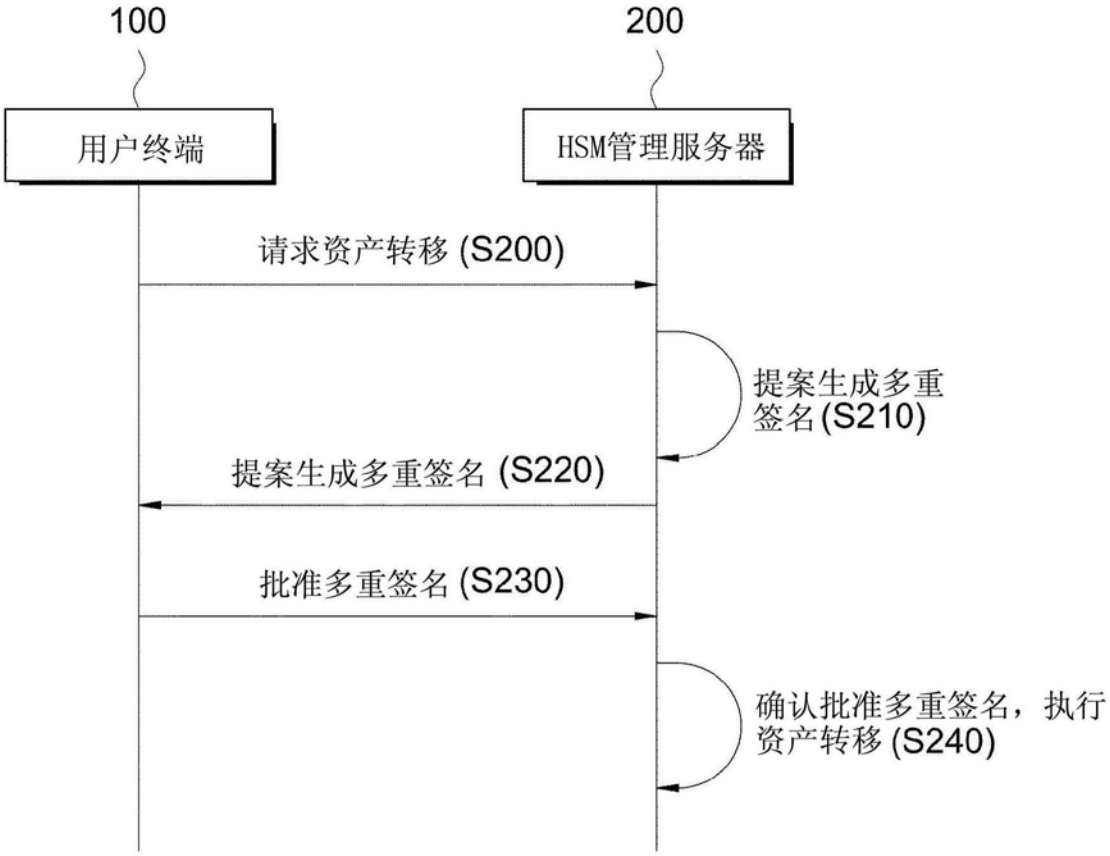

100
200
用户终端
HSM管理服务器
请求资产转移 (S200)
提案生成多重签名(S210)
提案生成多重签名 (S220)
批准多重签名 (S230)
确认批准多重签名，执行资产转移 (S240)

图3

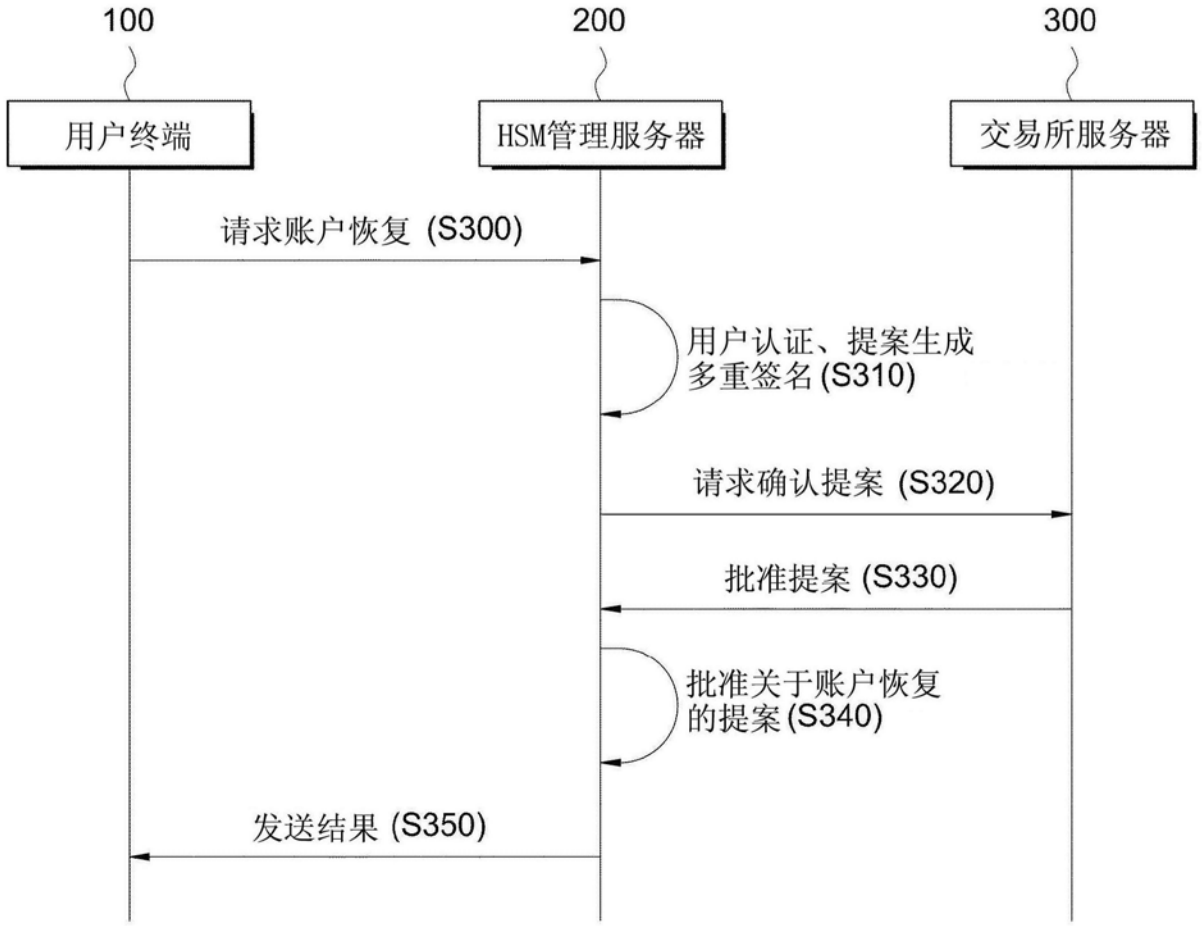

100
200
300
用户终端
HSM管理服务器
交易所服务器
请求账户恢复 (S300)
用户认证、提案生成
多重签名(S310)
请求确认提案 (S320)
批准提案 (S330)
批准关于账户恢复
的提案(S340)
发送结果 (S350)

图4