(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112564915 B
(45)授权公告日 2023.05.09

(21)申请号 202011367235.6
(22)申请日 2020.11.27
(65)同一申请的已公布的文献号
申请公布号 CN 112564915 A
(43)申请公布日 2021.03.26
(73)专利权人 中国联合网络通信集团有限公司
地址 100033 北京市西城区金融大街21号
(72)发明人 肖征荣 白琳 邢建兵 田新雪
(74)专利代理机构 北京天昊联合知识产权代理有限公司 11112
专利代理师 彭瑞欣 冯建基
(51)Int.Cl.
H04L 9/32(2006.01)

(56)对比文件
CN 105450403 A,2016.03.30
CN 105227305 A,2016.01.06
JP 2012173992 A,2012.09.10
CN 108848278 A,2018.11.20
CN 107438059 A,2017.12.05
CN 111835765 A,2020.10.27

审查员 姚雅倩

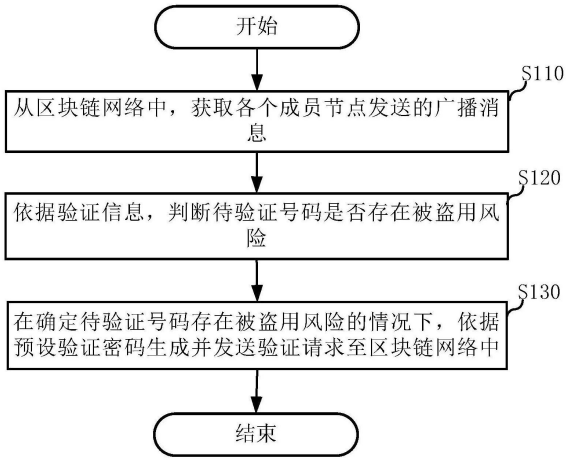
权利要求书4页 说明书11页 附图4页

(54)发明名称

验证方法和一号多终端管理服务器、终端

(57)摘要

本申请公开了一种验证方法和一号多终端管理服务器、终端。方法包括：从区块链网络中，获取各个成员节点发送的广播消息，其中，广播消息包括验证信息；依据验证信息，判断待验证号码是否存在被盗用风险；在确定待验证号码存在被盗用风险的情况下，依据预设验证密码生成并发送验证请求至区块链网络中，以使一号多终端中的副卡终端对主卡终端进行验证，并获得验证结果。通过预设验证密码，使一号多终端中的副卡终端对主卡终端进行验证，以确定主卡终端是否处于安全状态，避免用户的身份信息泄露而导致的用户财产损失，保障用户信息和财产的安全，提升用户体验度。



CN 112564915 B

1.一种验证方法,其特征在于,应用于一号多终端管理服务器,所述方法包括:

从区块链网络中,获取各个成员节点发送的广播消息,其中,所述广播消息包括验证信息;

依据所述验证信息,判断待验证号码是否存在被盗用风险;

在确定所述待验证号码存在被盗用风险的情况下,依据预设验证密码生成并发送验证请求至所述区块链网络中,以使一号多终端中的副卡终端对主卡终端进行验证,并获得验证结果;

其中,所述验证信息包括社保信息、银行监管信息、网络贷款信息和运营商信息中的任意一种或几种;

其中,所述依据所述验证信息,判断待验证号码是否存在被盗用风险,包括:

依据所述社保信息判断所述待验证号码是否登录过社保平台并获取与所述待验证号码对应的身份证信息,获得第一判断结果;

依据所述银行监管信息判断所述待验证号码是否登录过银行系统并进行金融交易,获得第二判断结果;

依据所述网络贷款信息判断所述待验证号码是否进行过网络贷款操作,获得第三判断结果;

依据所述运营商信息判断所述待验证号码是否与所述银行系统或网络贷款系统发生过通信,获得第四判断结果;

依据所述第一判断结果、所述第二判断结果、所述第三判断结果和所述第四判断结果中的任意一种或几种,判断所述待验证号码是否存在被盗用风险;

其中,所述从区块链网络中,获取各个成员节点发送的广播消息之前,还包括:

获取所述待验证号码的挂失信息和解挂信息,其中,所述挂失信息包括所述待验证号码对应的挂失终端的设备标识,所述解挂信息包括所述待验证号码对应的解挂终端的设备标识。

2.根据权利要求1所述的方法,其特征在于,所述运营商信息包括:通信短消息信息、通话记录信息和网络消息中的任意一种或几种。

3.根据权利要求1所述的方法,其特征在于,所述在确定所述待验证号码存在被盗用风险的情况下,依据预设验证密码生成并发送验证请求至所述区块链网络中之后,还包括:

在确定所述验证结果为所述主卡终端是非法终端的情况下,限制所述主卡终端的使用权限。

4.根据权利要求3所述的方法,其特征在于,所述在确定所述验证结果为所述主卡终端是非法终端的情况下,限制所述主卡终端的使用权限,包括:

依据所述验证结果,生成所述主卡终端的被盗用标识;

依据所述主卡终端的设备标识和所述被盗用标识,生成告警消息;

发送所述告警消息至所述区块链网络中,以使各个所述成员节点对所述主卡终端对应的账户进行冻结。

5.根据权利要求1所述的方法,其特征在于,所述挂失信息还包括所述挂失终端的位置信息和所述挂失终端的通信信息中的任意一种或几种;所述解挂信息还包括所述解挂终端的位置信息和所述解挂终端的通信信息中的任意一种或几种。

6.一种终端的验证方法，其特征在于，应用于一号多终端中的副卡终端，所述方法包括：

从区块链网络中，获取一号多终端管理服务器发送的验证请求，所述验证请求包括预设验证密码；其中，所述验证请求由所述一号多终端管理服务器通过以下方式发送：从区块链网络中，获取各个成员节点发送的广播消息，其中，所述广播消息包括验证信息；依据所述验证信息，判断待验证号码是否存在被盗用风险；在确定所述待验证号码存在被盗用风险的情况下，依据预设验证密码生成并发送验证请求至所述区块链网络中；

依据所述预设验证密码对主卡终端进行验证，获得验证结果；

依据所述验证结果，生成并发送验证响应至区块链网络中，以使所述一号多终端管理服务器限制所述主卡终端的使用权限；

其中，所述验证信息包括社保信息、银行监管信息、网络贷款信息和运营商信息中的任意一种或几种；

其中，所述依据所述验证信息，判断待验证号码是否存在被盗用风险，包括：

依据所述社保信息判断所述待验证号码是否登录过社保平台并获取与所述待验证号码对应的身份证信息，获得第一判断结果；

依据所述银行监管信息判断所述待验证号码是否登录过银行系统并进行金融交易，获得第二判断结果；

依据所述网络贷款信息判断所述待验证号码是否进行过网络贷款操作，获得第三判断结果；

依据所述运营商信息判断所述待验证号码是否与所述银行系统或网络贷款系统发生过通信，获得第四判断结果；

依据所述第一判断结果、所述第二判断结果、所述第三判断结果和所述第四判断结果中的任意一种或几种，判断所述待验证号码是否存在被盗用风险；

其中，所述从区块链网络中，获取各个成员节点发送的广播消息之前，还包括：

获取所述待验证号码的挂失信息和解挂信息，其中，所述挂失信息包括所述待验证号码对应的挂失终端的设备标识，所述解挂信息包括所述待验证号码对应的解挂终端的设备标识。

7.根据权利要求6所述的方法，其特征在于，所述依据所述预设验证密码对主卡终端进行验证，获得验证结果，包括：

从区块链网络中，获取主卡终端发送的待验证哈希值，所述待验证哈希值是所述主卡终端对待验证密码进行哈希运算，获得的哈希值；

对当前终端预先保存的预设密码进行哈希运算，获得预设哈希值；

依据所述预设哈希值和所述待验证哈希值，确定所述验证结果。

8.一种一号多终端管理服务器，其特征在于，其包括：

第一获取模块，用于从区块链网络中，获取各个成员节点发送的广播消息，其中，所述广播消息包括验证信息；

判断模块，用于依据所述验证信息，判断待验证号码是否存在被盗用风险；

第一验证模块，用于在确定所述待验证号码存在被盗用风险的情况下，依据预设验证密码生成并发送验证请求至所述区块链网络中，以使一号多终端中的副卡终端对主卡终端

进行验证，并获得验证结果；

其中，所述验证信息包括社保信息、银行监管信息、网络贷款信息和运营商信息中的任意一种或几种；

其中，所述依据所述验证信息，判断待验证号码是否存在被盗用风险，包括：

依据所述社保信息判断所述待验证号码是否登录过社保平台并获取与所述待验证号码对应的身份证信息，获得第一判断结果；

依据所述银行监管信息判断所述待验证号码是否登录过银行系统并进行金融交易，获得第二判断结果；

依据所述网络贷款信息判断所述待验证号码是否进行过网络贷款操作，获得第三判断结果；

依据所述运营商信息判断所述待验证号码是否与所述银行系统或网络贷款系统发生过通信，获得第四判断结果；

依据所述第一判断结果、所述第二判断结果、所述第三判断结果和所述第四判断结果中的任意一种或几种，判断所述待验证号码是否存在被盗用风险；

其中，所述从区块链网络中，获取各个成员节点发送的广播消息之前，还包括：

获取所述待验证号码的挂失信息和解挂信息，其中，所述挂失信息包括所述待验证号码对应的挂失终端的设备标识，所述解挂信息包括所述待验证号码对应的解挂终端的设备标识。

9.一种一号多终端中的副卡终端，其特征在于，其包括：

第二获取模块，用于从区块链网络中，获取一号多终端管理服务器发送的验证请求，所述验证请求包括预设验证密码；其中，所述验证请求由所述一号多终端管理服务器通过以下方式发送：从区块链网络中，获取各个成员节点发送的广播消息，其中，所述广播消息包括验证信息；依据所述验证信息，判断待验证号码是否存在被盗用风险；在确定所述待验证号码存在被盗用风险的情况下，依据预设验证密码生成并发送验证请求至所述区块链网络中；

第二验证模块，用于依据所述预设验证密码对主卡终端进行验证，获得验证结果；

处理模块，用于依据所述验证结果，生成并发送验证响应至所述区块链网络中，以使所述一号多终端管理服务器限制所述主卡终端的使用权限；

其中，所述验证信息包括社保信息、银行监管信息、网络贷款信息和运营商信息中的任意一种或几种；

其中，所述依据所述验证信息，判断待验证号码是否存在被盗用风险，包括：

依据所述社保信息判断所述待验证号码是否登录过社保平台并获取与所述待验证号码对应的身份证信息，获得第一判断结果；

依据所述银行监管信息判断所述待验证号码是否登录过银行系统并进行金融交易，获得第二判断结果；

依据所述网络贷款信息判断所述待验证号码是否进行过网络贷款操作，获得第三判断结果；

依据所述运营商信息判断所述待验证号码是否与所述银行系统或网络贷款系统发生过通信，获得第四判断结果；

依据所述第一判断结果、所述第二判断结果、所述第三判断结果和所述第四判断结果中的任意一种或几种，判断所述待验证号码是否存在被盗用风险；

其中，所述从区块链网络中，获取各个成员节点发送的广播消息之前，还包括：

获取所述待验证号码的挂失信息和解挂信息，其中，所述挂失信息包括所述待验证号码对应的挂失终端的设备标识，所述解挂信息包括所述待验证号码对应的解挂终端的设备标识。

验证方法和一号多终端管理服务器、终端

技术领域

[0001] 本申请涉及通信技术领域，具体涉及一种验证方法和一号多终端管理服务器、终端。

背景技术

[0002] 目前，用户所使用的智能终端(例如，智能手机等)多具有网络支付功能，用户还会将自己的身份信息与该智能终端绑定，用以验证在网络支付的情况下的身份验证。

[0003] 但是，如果用户的智能手机被盗或丢失，而刚好电信运营商的营业厅处于停业状态(例如，营业厅下班)时，会导致用户无法及时补卡；虽然可以采用打电话的方式对手机号码进行挂失处理，但是，第三方仍可以通过打电话的方式对手机号码进行解挂处理，这样会导致用户的手机号码仍然处于被盗用状态，使犯罪分子会有一整晚的时间进行犯罪活动，例如，通过手机号码来获得被盗用户的身份信息，导致用户的身份信息泄露；或通过手机的网络支付功能购买商品，造成被盗用户的财产损失。

发明内容

[0004] 为此，本申请提供一种验证方法和一号多终端管理服务器、终端，如何在终端被盗用的情况下，保障用户信息和财产的安全性的问题。

[0005] 为了实现上述目的，本申请第一方面提供一种验证方法，方法包括：从区块链网络中，获取各个成员节点发送的广播消息，其中，广播消息包括验证信息；依据验证信息，判断待验证号码是否存在被盗用风险；在确定待验证号码存在被盗用风险的情况下，依据预设验证密码生成并发送验证请求至区块链网络中，以使一号多终端中的副卡终端对主卡终端进行验证，并获得验证结果。

[0006] 在一个具体实现中，验证信息包括社保信息、银行监管信息、网络贷款信息和运营商信息中的任意一种或几种。

[0007] 在一个具体实现中，依据验证信息，判断待验证号码是否存在被盗用风险，包括：依据社保信息判断待验证号码是否登录过社保平台并获取与待验证号码对应的身份证信息，获得第一判断结果；依据银行监管信息判断待验证号码是否登录过银行系统并进行金融交易，获得第二判断结果；依据网络贷款信息判断待验证号码是否进行过网络贷款操作，获得第三判断结果；依据运营商信息判断待验证号码是否与银行系统或网络贷款系统发生过通信，获得第四判断结果；依据第一判断结果、第二判断结果、第三判断结果和第四判断结果中的任意一种或几种，判断待验证号码是否存在被盗用风险。

[0008] 在一个具体实现中，运营商信息包括：通信短消息信息、通话记录信息和网络消息中的任意一种或几种。

[0009] 在一个具体实现中，在确定待验证号码存在被盗用风险的情况下，依据预设验证密码生成并发送验证请求至区块链网络中之后，还包括：在确定验证结果为主卡终端是非法终端的情况下，限制主卡终端的使用权限。

[0010] 在一个具体实现中，在确定验证结果为主卡终端是非法终端的情况下，限制主卡终端的使用权限，包括：依据验证结果，生成主卡终端的被盗用标识；依据主卡终端的设备标识和被盗用标识，生成告警消息；发送告警消息至区块链网络中，以使各个成员节点对主卡终端对应的账户进行冻结。

[0011] 在一个具体实现中，从区块链网络中，获取各个成员节点发送的广播消息之前，还包括：获取待验证号码的挂失信息和解挂信息；其中，挂失信息包括待验证号码对应的挂失终端的设备标识，解挂信息包括待验证号码对应的解挂终端的设备标识。

[0012] 在一个具体实现中，挂失信息还包括挂失终端的位置信息和挂失终端的通信信息中的任意一种或几种；解挂信息还包括解挂终端的位置信息和解挂终端的通信信息中的任意一种或几种。

[0013] 为了实现上述目的，本申请第二方面提供一种终端的验证方法，方法包括：从区块链网络中，获取一号多终端管理服务器发送的验证请求，验证请求包括预设验证密码；依据预设验证密码对主卡终端进行验证，获得验证结果；依据验证结果，生成并发送验证响应至区块链网络中，以使一号多终端管理服务器限制主卡终端的使用权限。

[0014] 在一个具体实现中，依据预设验证密码对主卡终端进行验证，获得验证结果，包括：从区块链网络中，获取主卡终端发送的待验证哈希值，待验证哈希值是主卡终端对待验证密码进行哈希运算，获得的哈希值；对当前终端预先保存的预设密码进行哈希运算，获得预设哈希值；依据预设哈希值和待验证哈希值，确定验证结果。

[0015] 为了实现上述目的，本申请第三方面提供一种一号多终端管理服务器，其包括：第一获取模块，用于从区块链网络中，获取各个成员节点发送的广播消息，其中，广播消息包括验证信息；判断模块，用于依据验证信息，判断待验证号码是否存在被盗用风险；第一验证模块，用于在确定待验证号码存在被盗用风险的情况下，依据预设验证密码生成并发送验证请求至区块链网络中，以使一号多终端中的副卡终端对主卡终端进行验证，并获得验证结果。

[0016] 为了实现上述目的，本申请第四方面提供一种终端，其包括：

[0017] 第二获取模块，用于从区块链网络中，获取一号多终端管理服务器发送的验证请求，验证请求包括预设验证密码；第二验证模块，用于依据预设验证密码对主卡终端进行验证，获得验证结果；处理模块，用于依据验证结果，生成并发送验证响应至区块链网络中，以使一号多终端管理服务器限制主卡终端的使用权限。

[0018] 本申请中的验证方法和一号多终端管理服务器、终端，通过依据验证信息，判断待验证号码是否存在被盗用风险，全面衡量待验证号码的安全性；在确定待验证号码存在被盗用风险的情况下，依据预设验证密码生成并发送验证请求至区块链网络中，以使一号多终端中的副卡终端对主卡终端进行验证，并获得验证结果。通过预设验证密码，使一号多终端中的副卡终端对主卡终端进行验证，以确定主卡终端是否处于安全状态，避免用户的身份信息泄露而导致的用户财产损失，保障用户信息和财产的安全，提升用户体验度。

附图说明

[0019] 附图用来提供对本公开实施例的进一步理解，并且构成说明书的一部分，与本公开的实施例一起用于解释本公开，并不构成对本公开的限制。通过参考附图对详细示例实

施例进行描述，以上和其它特征和优点对本领域技术人员将变得更加显而易见，在附图中：

[0020] 图1示出本申请一实施例中的验证方法的流程示意图。

[0021] 图2示出本申请又一实施例中的验证方法的流程示意图。

[0022] 图3示出本申请实施例中的终端的验证方法的流程示意图。

[0023] 图4示出本申请实施例中的一号多终端管理服务器的组成方框图。

[0024] 图5示出本申请实施例中的终端的组成方框图。

[0025] 图6示出本申请实施例中的验证系统的组成方框图。

[0026] 图7示出本申请实施例中的验证系统的工作方法的流程示意图。

[0027] 在附图中：

[0028] 401:第一获取模块 402:判断模块

[0029] 403:第一验证模块 501:第二获取模块

[0030] 502:第二验证模块 503:处理模块

[0031] 610:验证服务器 611:用户号码安全保障节点服务器

[0032] 612:一号多终端管理服务器 620:主卡终端

[0033] 630:副卡终端 640:社保节点服务器

[0034] 650:银行监管节点服务器 660:网贷平台监管节点服务器

[0035] 670:运营商节点服务器 671:运营商短信息节点服务器

[0036] 672:运营商核心网节点服务器 673:用户行为分析节点服务器

具体实施方式

[0037] 以下结合附图对本申请的具体实施方式进行详细说明。应当理解的是，此处所描述的具体实施方式仅用于说明和解释本申请，并不用于限制本申请。对于本领域技术人员来说，本申请可以在不需要这些具体细节中的一些细节的情况下实施。下面对实施例的描述仅仅是为了通过示出本申请的示例来提供对本申请更好的理解。

[0038] 需要说明的是，在本文中，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……”限定的要素，并不排除在包括要素的过程、方法、物品或者设备中还存在另外的相同要素。

[0039] 为使本申请的目的、技术方案和优点更加清楚，下面将结合附图对本申请实施方式作进一步地详细描述。

[0040] 图1示出本申请一实施例中的验证方法的流程示意图。该验证方法可应用于一号多终端管理服务器。如图1所示，验证方法包括如下步骤：

[0041] 步骤S110，从区块链网络中，获取各个成员节点发送的广播消息。

[0042] 其中，广播消息包括验证信息。验证信息包括社保信息、银行监管信息、网络贷款信息和运营商信息中的任意一种或几种。

[0043] 例如，社保信息可以是社会保障体系服务器中与待验证号码相关的信息，银行监管信息可以是与待验证号码对应的银行账户信息、待验证号码在银行客户端所进行相关操作等信息，网络贷款信息可以是待验证号码对应的在网络贷款平台上所获取的贷款账号或

贷款额度等信息，运营商信息可以包括通话记录信息、短消息和核心网设备下发的通信网络配置信息中的任意一种或几种。以上对于验证信息仅是举例说明，可根据实际情况进行具体设定，其他未说明的验证信息也在本申请的保护范围之内，在此不再赘述。

[0044] 其中的待验证号码是用户所使用的手机号码或与用户的身份信息绑定的、无线网络运营商发布的通信设备的标识等。例如，国际移动用户识别码(International Mobile Subscriber Identity，IMSI)、临时移动用户识别码(Temporary Mobile Subscriber Identity，TMSI)等。

[0045] 步骤S120，依据验证信息，判断待验证号码是否存在被盗用风险。

[0046] 通过验证信息来验证待验证号码当前所处的状态，若验证信息中包括风险信息(例如，待验证号码最近频繁(例如，1小时登录一次)登录金融系统，进行转账或汇款等行为)，则确定待验证号码存在被盗用风险；否则，确定待验证号码是安全的，可以进行正常的通信。

[0047] 在一个具体实现中，依据验证信息，判断待验证号码是否存在被盗用风险，包括：依据社保信息判断待验证号码是否登录过社保平台并获取与待验证号码对应的身份证信息，获得第一判断结果；依据银行监管信息判断待验证号码是否登录过银行系统并进行金融交易，获得第二判断结果；依据网络贷款信息判断待验证号码是否进行过网络贷款操作，获得第三判断结果；依据运营商信息判断待验证号码是否接收过银行系统或网络贷款系统发送的验证信息，获得第四判断结果；依据第一判断结果、第二判断结果、第三判断结果和第四判断结果中的任意一种或几种，判断待验证号码是否存在被盗用风险。

[0048] 其中，第一判断结果包括：待验证号码登录过社保平台并获取与待验证号码对应的身份证信息，或，待验证号码没有登录过社保平台。第二判断结果包括：待验证号码登录过银行系统并进行金融交易，或，待验证号码没有登录过银行系统，没有进行任何金融交易。第三判断结果包括：待验证号码进行过网络贷款操作(例如，通过某网贷平台申请过贷款等)，或，待验证号码没有进行过任何网络贷款操作。第四判断结果包括：待验证号码接收过银行系统或网络贷款系统发送的验证信息，或，待验证号码没有接收过银行系统或网络贷款系统发送的验证信息。通过以上四种不同维度的判断结果，可全面的判断待验证号码是否存在被盗用风险，避免待验证号码对应的用户信息泄露，保证待验证号码的信息安全。

[0049] 步骤S130，在确定待验证号码存在被盗用风险的情况下，依据预设验证密码生成并发送验证请求至区块链网络中。

[0050] 一号多终端业务中的副卡终端从区块链网络中获取到验证请求，并通过对验证请求进行消息解析获得预设验证密码，依据该预设验证密码和主卡终端本地保存的待验证密码，确定验证结果，例如，当验证结果是待验证密码和预设验证密码相同时，表征对主卡终端验证通过；当验证结果是待验证密码和预设验证密码不同时，表征对主卡终端验证失败，即主卡终端是被盗用的终端。

[0051] 在本实施例中，通过依据验证信息，判断待验证号码是否存在被盗用风险，全面衡量待验证号码的安全性；在确定待验证号码存在被盗用风险的情况下，依据预设验证密码生成并发送验证请求至区块链网络中，以使一号多终端中的副卡终端对主卡终端进行验证，并获得验证结果。通过预设验证密码，使一号多终端中的副卡终端对主卡终端进行验证，以确定主卡终端是否处于安全状态，避免用户的身份信息泄露而导致的用户财产损失，

保障用户信息和财产的安全，提升用户体验度。

[0052] 在一个具体实现中，从区块链网络中，获取各个成员节点发送的广播消息之前，还包括：获取待验证号码的挂失信息和解挂信息；其中，挂失信息包括待验证号码对应的挂失终端的设备标识，解挂信息包括待验证号码对应的解挂终端的设备标识。

[0053] 其中，挂失信息是终端登陆运营商节点服务器，对待验证号码进行挂失处理的过程中所产生的信息。例如，挂失信息包括待验证号码对应的挂失终端的设备标识(例如，终端的出厂编号等)，挂失终端的位置信息和挂失终端的通信信息中的任意一种或几种。

[0054] 解挂信息是终端登陆运营商节点服务器，对待验证号码进行解除挂失处理的过程中所产生的信息。例如，解挂信息包括待验证号码对应的解挂终端的设备标识、解挂终端的位置信息和解挂终端的通信信息中的任意一种或几种。

[0055] 通过获取待验证号码的挂失信息和解挂信息，来确定待验证号码是否在预设时长(例如，4个小时内)内，仅进行了挂失处理，又进行了解挂处理。若确定在预设时长内，待验证号码先进行了挂失，然后又进行了解挂，可能存在待验证号码对应的终端丢失的风险，该待验证号码对应的终端可能被第三方获取到，易导致待验证号码对应的用户的身份信息泄露，或，用户的财产被盗取的风险。将存在被盗取风险的待验证号码标注处理，有利于对待验证号码做进一步的验证，以保证待验证号码对应的用户的信息安全和财产安全，提高用户体验度。

[0056] 图2示出本申请又一实施例中的验证方法的流程示意图。该验证方法可应用于一号多终端管理服务器。如图2所示，验证方法包括如下步骤：

[0057] 步骤S210，从区块链网络中，获取各个成员节点发送的广播消息。

[0058] 步骤S220，依据验证信息，判断待验证号码是否存在被盗用风险；

[0059] 步骤S230，在确定待验证号码存在被盗用风险的情况下，依据预设验证密码生成并发送验证请求至区块链网络中。

[0060] 需要说明的是，本实施例中的步骤S210～步骤S230，与上一实施例中的步骤S110～步骤S130相同，在此不再赘述。

[0061] 步骤S240，在确定验证结果为主卡终端是非法终端的情况下，限制主卡终端的使用权限。

[0062] 其中，限制主卡终端的使用权限可以包括：限制主卡终端的正常通信功能、冻结主卡终端中的待验证号码对应的金融账号、暂停待验证号码对应的信贷账号和限制待验证号码对应的设保服务功能中的任意一种或几种。以上对于主卡终端的使用权限仅是举例说明，可根据具体情况进行具体设定，其他未说明的主卡终端的使用权限也在本申请的保护范围之内，在此不再赘述。

[0063] 在一个具体实现中，在确定验证结果为主卡终端是非法终端的情况下，限制主卡终端的使用权限，包括：依据验证结果，生成主卡终端的被盗用标识；依据主卡终端的设备标识和被盗用标识，生成告警消息；发送告警消息至区块链网络中，以使各个成员节点对主卡终端对应的账户进行冻结。

[0064] 其中，被盗用标识表征主卡终端是已经丢失的终端，并且该主卡终端可能被第三方获取到，因智能终端多具有移动网络支付功能，或与该智能终端对应的被盗用的用户的身份信息绑定，第三方可通过该主卡终端进行金融操作，例如，通过网络购买行为，消耗被

盗用的用户的财产，导致被盗用的用户的身份信息泄露等。通过发送告警消息至区块链网络中，可使区块链网络中的各个成员节点都能获知该主卡终端已经被盗用，将该主卡终端对应的账号进行冻结，避免被盗用的用户的财产损失，保证被盗用的用户的权益。

[0065] 在本实施例中，通过依据验证信息，判断待验证号码是否存在被盗用风险，全面衡量待验证号码的安全性；在确定待验证号码存在被盗用风险的情况下，依据预设验证密码生成并发送验证请求至区块链网络中，以使一号多终端中的副卡终端对主卡终端进行验证，并获得验证结果。通过预设验证密码，使一号多终端中的副卡终端对主卡终端进行验证，以确定主卡终端是否处于安全状态，在确定该主卡终端是非法终端的情况下，限制主卡终端的使用权限，避免用户的身份信息泄露而导致的用户财产损失，保障用户信息和财产的安全，提升用户体验度。

[0066] 图3示出本申请实施例中的终端的验证方法的流程示意图。该终端的验证方法可应用于一号多终端业务中的副卡终端。如图3所示，该终端的验证方法包括如下步骤：

[0067] 步骤S310，从区块链网络中，获取一号多终端管理服务器发送的验证请求。

[0068] 其中，验证请求包括预设验证密码。

[0069] 步骤S320，依据预设验证密码对主卡终端进行验证，获得验证结果。

[0070] 其中，预设验证密码是预先保存的用户预先设置的密码，而主卡终端自己本地也保存有一份待验证密码，通过待验证密码和预设验证密码，可确定验证结果。例如，验证结果可以是待验证密码和预设验证密码相同，即对主卡终端验证通过；验证结果还可以是待验证密码和预设验证密码不同，即对主卡终端验证失败，主卡终端是被盗用的终端。

[0071] 在一个具体实现中，依据预设验证密码对主卡终端进行验证，获得验证结果，包括：从区块链网络中，获取主卡终端发送的待验证哈希值，待验证哈希值是主卡终端对待验证密码进行哈希运算，获得的哈希值；对当前终端预先保存的预设密码进行哈希运算，获得预设哈希值；依据预设哈希值和待验证哈希值，确定验证结果。

[0072] 其中，通过主卡终端对待验证密码进行哈希运算，可保证待验证密码在区块链网络的传输过程中的安全性。通过对比预设哈希值和待验证哈希值来确定验证结果，这样即保证了主卡终端的信息安全性，也验证了主卡终端是否是被盗用的终端。提高终端的安全性。

[0073] 在一个具体实现中，若当前终端是主卡终端期望接收到该待验证哈希值的目的终端，当前终端可以通过待验证哈希值，反向推算获得待验证密码，但是，若当前终端不是主卡终端期望接收到该待验证哈希值的目的终端，则当前终端是无法依据待验证哈希值确定待验证密码的，避免待验证密码被第三方设备接收到，保证主卡终端的信息安全性。

[0074] 步骤S330，依据验证结果，生成并发送验证响应至区块链网络中。

[0075] 当一号多终端管理服务器从区块链网络中获取到验证响应时，可通过对验证响应的解析，获得验证结果。若验证结果为待验证密码与预设密码不同时，可确定对主卡终端验证失败，确定主卡终端所使用的待验证号码是被盗用的号码，通过一号多终端管理服务器限制主卡终端的使用权限，避免被盗用的用户的财产损失。若验证结果为待验证密码与预设密码相同时，可确定对主卡终端验证成功，一号多终端管理服务器会发送验证成功消息给运营商核心网节点服务器，以使主卡终端可以进行正常使用待验证号码，保证待验证号码的正常通信。

[0076] 在本实施例中，通过从区块链网络中，获取一号多终端管理服务器发送的预设验证密码，并依据该预设验证密码对主卡终端进行验证，当待验证密码与预设密码不同时，可确定对主卡终端验证失败，确定主卡终端所使用的待验证号码是被盗用的号码，通过一号多终端管理服务器限制主卡终端的使用权限，保证被盗用的用户权益，避免用户的信息泄露和财产损失，提高用户的安全性。

[0077] 图4示出本申请实施例中的一号多终端管理服务器的组成方框图。如图4所示，该一号多终端管理服务器具体包括如下模块：

[0078] 第一获取模块401，用于从区块链网络中，获取各个成员节点发送的广播消息，其中，广播消息包括验证信息；判断模块402，用于依据验证信息，判断待验证号码是否存在被盗用风险；第一验证模块403，用于在确定待验证号码存在被盗用风险的情况下，依据预设验证密码生成并发送验证请求至区块链网络中，以使一号多终端中的副卡终端对主卡终端进行验证，并获得验证结果。

[0079] 在本实施例中，通过判断模块依据验证信息，判断待验证号码是否存在被盗用风险，全面衡量待验证号码的安全性，避免待验证号码被盗用；第一验证模块在确定待验证号码存在被盗用风险的情况下，依据预设验证密码生成并发送验证请求至区块链网络中，以使一号多终端中的副卡终端对主卡终端进行验证，并获得验证结果。通过预设验证密码，使一号多终端中的副卡终端对主卡终端进行验证，以确定主卡终端是否处于安全状态，避免用户的身份信息泄露，进而导致的用户财产损失，保障用户信息和财产的安全，提升用户体验度。

[0080] 图5示出本申请实施例中的终端的组成方框图。该终端可以是一号多终端业务中的副卡终端。如图5所示，该终端具体包括如下模块：

[0081] 第二获取模块501，用于从区块链网络中，获取一号多终端管理服务器发送的验证请求，验证请求包括预设验证密码；第二验证模块502，用于依据预设验证密码对主卡终端进行验证，获得验证结果；处理模块503，用于依据验证结果，生成并发送验证响应至区块链网络中，以使一号多终端管理服务器限制主卡终端的使用权限。

[0082] 在本实施例中，通过第二获取模块从区块链网络中，获取一号多终端管理服务器发送的预设验证密码，并使用第二验证模块依据该预设验证密码对主卡终端进行验证，当待验证密码与预设密码不同时，可确定对主卡终端验证失败，确定主卡终端所使用的待验证号码是被盗用的号码，通过处理模块依据验证结果生成并发送验证响应至区块链网络中，使一号多终端管理服务器限制主卡终端的使用权限，保证被盗用的用户权益，避免用户的信息泄露和财产损失，提高用户的安全性。

[0083] 值得一提的是，本实施方式中所涉及到的各模块均为逻辑模块，在实际应用中，一个逻辑单元可以是一个物理单元，也可以是一个物理单元的一部分，还可以以多个物理单元的组合实现。此外，为了突出本申请的创新部分，本实施方式中并没有将与解决本申请所提出的技术问题关系不太密切的单元引入，但这并不表明本实施方式中不存在其它的单元。

[0084] 图6示出本申请实施例中的验证系统的组成方框图。如图6所示，具体包括如下设备：验证服务器610、主卡终端620、副卡终端630、社保节点服务器640、银行监管节点服务器650、网贷平台监管节点服务器660和运营商节点服务器670。其中，验证服务器610包括：用

户号码安全保障节点服务器611和一号多终端管理服务器612。运营商节点服务器670包括：运营商短信息节点服务器671、运营商核心网节点服务器672和用户行为分析节点服务器623。

[0085] 图7示出本申请实施例中的验证系统的工作方法的流程示意图。如图7所示，具体包括如下步骤。

[0086] 步骤S701，副卡终端630登陆运营商节点服务器670，对该副卡终端630对应的待验证号码进行挂失。

[0087] 例如，副卡终端630可通过致电运营商客服电话(如10010/10000/10086等)，或者通过副卡终端630的手机客户端(如手机营业厅)等登录运营商节点服务器670，进行待验证号码的挂失处理，生成挂失信息。其中，挂失信息包括副卡终端630的设备标识、副卡终端630的位置信息(例如，经纬度信息等)和副卡终端630的通信信息中的任意一种或几种。

[0088] 例如，副卡终端630的通信信息包括副卡终端630所处的基站小区信息(如，物理小区标识(Physical Cell Identifier，PCI)等)和副卡终端630对应的IMSI等。

[0089] 步骤S702，主卡终端620登陆运营商节点服务器670，对待验证号码进行解挂操作。

[0090] 例如，主卡终端620可通过致电运营商客服电话(如10010/10000/10086等)，或者通过主卡终端620的手机客户端(如手机营业厅)等登录运营商节点服务器670，进行待验证号码的解挂处理。其中，解挂信息包括主卡终端620的设备标识、主卡终端620的位置信息(例如，经纬度信息等)和主卡终端620的通信信息中的任意一种或几种。

[0091] 例如，主卡终端620的通信信息包括主卡终端620所处的基站小区信息(如，PCI等)和主卡终端620对应的IMSI等。

[0092] 步骤S703，运营商节点服务器670依据待验证号码的解挂信息和挂失信息，生成第一广播消息，并使用自己的私钥对第一广播消息进行签名，生成并发送签名后的第一广播消息至区块链网络中，以使验证服务器610获得第一广播消息。

[0093] 步骤S704，由于待验证号码即进行了挂失处理，也进行了解挂处理，并且这两个处理过程是不同终端执行的，验证服务器610中的用户号码安全保障节点服务器611将待验证号码标注为存在盗用风险的手机号码，启动对待验证号码的监控操作，以防止待验证号码被盗用。例如，用户号码安全保障节点服务器611依据待验证号码(如186xxxx8888)、挂失信息和解挂信息，生成第二广播消息，

[0094] 步骤S705，用户号码安全保障节点服务器611对第二广播消息进行私钥签名，生成并发送签名后的第二广播消息到区块链网络中。

[0095] 步骤S706，运营商节点服务器670中的运营商核心网节点服务器672接收到第二广播消息，先对第二广播消息的私钥签名进行验证，在验证通过之后，获得待验证号码(如18611118888)、待验证号码的挂失信息和解挂信息，然后在对以上信息进行私钥签名，生成并发送签名后的第三广播消息到区块链网络中，以使用户号码安全保障节点服务器611获得第三广播消息。

[0096] 例如，第三广播消息还可以包括运营商核心网节点服务器672对待验证号码的解挂信息，待验证号码最后登录注册网络的网络信息等信息。

[0097] 需要说明的是，运营商节点服务器670中的运营商短信息节点服务器671接收到第三广播消息，对其私钥签名验证通过之后，获得待验证号码；依据待验证号码，调取待验证

号码对应的短消息记录;依据该短消息记录,判断待验证号码是否有向多个陌生号码发送短信,以及是否接收过多个银行发送的验证短消息或网贷平台发送的验证短消息等,获得判断结果;依据该判断结果和待验证号码,生成第四广播消息,并对该第四广播消息进行私钥签名,生成并发送签名后的第四广播消息到区块链网络中,以使用户号码安全保障节点服务器611获得第四广播消息。

[0098] 运营商节点服务器670中的用户行为分析节点服务器673接收到第三广播消息,对其私钥签名验证通过之后,获得待验证号码,依据待验证号码查找自己的内部数据库,获得第一查找结果,该第一查找结果包括待验证号码对应的通话记录;依据该通话记录,判断待验证号码是否进行过与多个陌生电话号码进行通话的情况;如果有,将通话记录信息进行私钥签名,生成并发送第五广播消息到区块链网络中,以使用户号码安全保障节点服务器611获得第五广播消息。

[0099] 步骤S707,社保节点服务器640接收到第三广播消息,对其私钥签名验证通过之后,获得待验证号码,社保节点服务器640依据待验证号码,查找自己的数据库,确定待验证号码是否登录过社保节点服务器640并获取与待验证号码对应的身份信息;若确定登陆过社保节点服务器640,则依据该待验证号码在社保节点服务器640上的操作信息、该操作信息对应的时间信息和待验证号码对应的身份信息,生成第六广播消息。并对该第六广播消息进行私钥签名,生成并发送签名后的第六广播消息到区块链网络中,以使用户号码安全保障节点服务器611获得第六广播消息。

[0100] 步骤S708,银行监管节点服务器650接收到第三广播消息,对其私钥签名验证通过之后,获得待验证号码,依据待验证号码查找自己的内部数据库,获得第二查找结果,该第二查找结果包括待验证号码是否登录过银行系统并进行的金融交易信息(例如,登录、注册、绑卡、转账等金融操作信息)信息,以及所进行的金融交易信息对应的时间信息。银行监管节点服务器650依据待验证号码、待验证号码对应的金融交易信息和金融交易信息对应的时间信息,生成第七广播消息,并使用自己的私钥对第七广播消息进行签名,生成并发送签名后的第七广播消息至区块链网络中,以使用户号码安全保障节点服务器611获得第七广播消息。

[0101] 步骤S709,网贷平台监管节点服务器660接收到第三广播消息,对其私钥签名验证通过之后,获得待验证号码,依据待验证号码查找自己的内部数据库,获得第三查找结果,该第三查找结果包括待验证号码是否进行过网络贷款操作,以及在进行网络贷款操作时的网贷操作信息(如登录、注册、贷款等操作的信息),以及所进行的网贷操作信息对应的时间信息。网贷平台监管节点服务器660依据待验证号码、待验证号码对应的网贷操作信息和网贷操作信息对应的时间信息,生成第八广播消息,并使用自己的私钥对第八广播消息进行签名,生成并发送签名后的第八广播消息至区块链网络中,以使用户号码安全保障节点服务器611获得第八广播消息。

[0102] 步骤S710,验证服务器610中的用户号码安全保障节点服务器611从区块链网络中,分别获得第三至八广播消息。分别对各个广播消息的私钥签名进行验证,在验证通过时,获得待验证号码。并依据待验证号码获取用户是否通过终端进行过登录社保节点服务器640获取身份证信息;是否登录银行监管节点服务器650进行相关操作;是否登录网贷平台监管节点服务器660进行注册和绑卡;是否接收到多个银行和网贷平台服务器发送的验

证短消息的操作信息等，依据以上各个操作信息和用户在对待验证号码进行挂失处理和解挂处理时所使用的用户终端设备的标识、位置信息、通话记录等信息进行判断。若确定以下条件中的任意一条或几条都成立：1)待验证号码有向多个陌生号码进行通话；2)有登录过多个网贷平台服务器或银行进行注册、刷卡等操作；3)在进行挂失处理和解挂处理的终端设备的标识与运营商核心网节点服务器672中存储的终端设备的标识不同，4)登录注册的小区信息不同，5)地理位置不同。则说明该待验证号码存在被盗用风险，生成待验证标识；依据该待验证标识，生成并发送验证消息给验证服务器610中的一号多终端管理服务器612。

[0103] 步骤S711，验证服务器610中的一号多终端管理服务器612从区块链网络中，获得验证消息；通过对验证消息的解析，获得待验证标识。依据该待验证标识，生成并分别发送认证请求给副卡终端630和主卡终端620，以使副卡终端630发起对主卡终端620的认证。

[0104] 步骤S712，主卡终端620对待验证密码进行哈希运算，获得待验证哈希值，并对该待验证哈希值进行私钥签名，生成签名后的待验证消息，发送签名后的待验证消息至区块链网络中，以使副卡终端630获得该待验证密码，并对该待验证密码进行验证。

[0105] 步骤S713，副卡终端630从区块链网络中，获得主卡终端620发送的待验证消息，先对该待验证消息的私钥签名进行验证，在验证通过时，获得待验证哈希值。同时，对预先保存的用户预先设置的预设密码进行哈希计算，获得预设哈希值；对比预设哈希值和待验证哈希值。当预设哈希值和待验证哈希值相同时，确定对主卡终端620验证通过；否则，确定对主卡终端620验证失败。

[0106] 步骤S714，当副卡终端630确定对主卡终端620验证失败时，副卡终端630生成验证失败标识；依据该验证失败标识和主卡终端620的设备标识，生成并发送验证失败消息至区块链网络中，以使一号多终端管理服务器612获得该验证失败标识。

[0107] 需要说明的是，当副卡终端630确定对主卡终端620验证成功时，一号多终端管理服务器612会发送验证成功消息给运营商核心网节点服务器672，以使主卡终端620可以进行正常使用待验证号码。

[0108] 步骤S715，一号多终端管理服务器612从区块链网络中获得验证失败消息，通过消息解析，获得验证失败标识和主卡终端620的设备标识，同时，生成主卡终端620被盗用标识；依据主卡终端620被盗用标识和主卡终端620的设备标识，生成并发送告警消息至区块链网络中，以使区块链网络中的各个节点对主卡终端620对应的账号进行冻结。

[0109] 例如，当银行监管节点服务器650和网贷平台监管节点服务器660从区块链网络中获得告警消息时，根据主卡终端620的设备标识，查找获得主卡终端620对应的金融账号，并将该金融账号进行冻结，以避免被盗用户的财产损失，提高用户的安全性。当运营商核心网节点服务器672从区块链网络中获得告警消息时，会停止主卡终端620的通信功能，并对主卡终端620进行锁定。当社保节点服务器640从区块链网络中获得告警消息时，会禁止主卡终端620对应的账号登录，以保证用户的身份信息的安全。

[0110] 在本实施例中，在营业厅下班时间内，一号多终端用户进行的挂失和解挂失的操作，如果用户已经进行了挂失，再通过其他手机号码进行解挂失，通过第三至第八广播消息中的各种验证信息，判断待验证号码是否存在被盗用风险，全面衡量待验证号码的安全性；在确定待验证号码存在被盗用风险的情况下，依据预设验证密码生成并发送验证请求至区

块链网络中，以使一号多终端中的副卡终端对主卡终端进行验证，并获得验证结果。通过预设验证密码，使一号多终端中的副卡终端对主卡终端进行验证，以确定主卡终端是否处于安全状态，在确定用户所使用的终端和待验证号码丢失的情况下，通过区块链网络中的各个节点对主卡终端对应的金融账号进行冻结，以避免被盗用户的财产损失，提高用户的安全性，提升用户体验度。

[0111] 可以理解的是，以上实施方式仅仅是为了说明本申请的原理而采用的示例性实施方式，然而本申请并不局限于此。对于本领域内的普通技术人员而言，在不脱离本申请的精神和实质的情况下，可以做出各种变型和改进，这些变型和改进也视为本申请的保护范围。

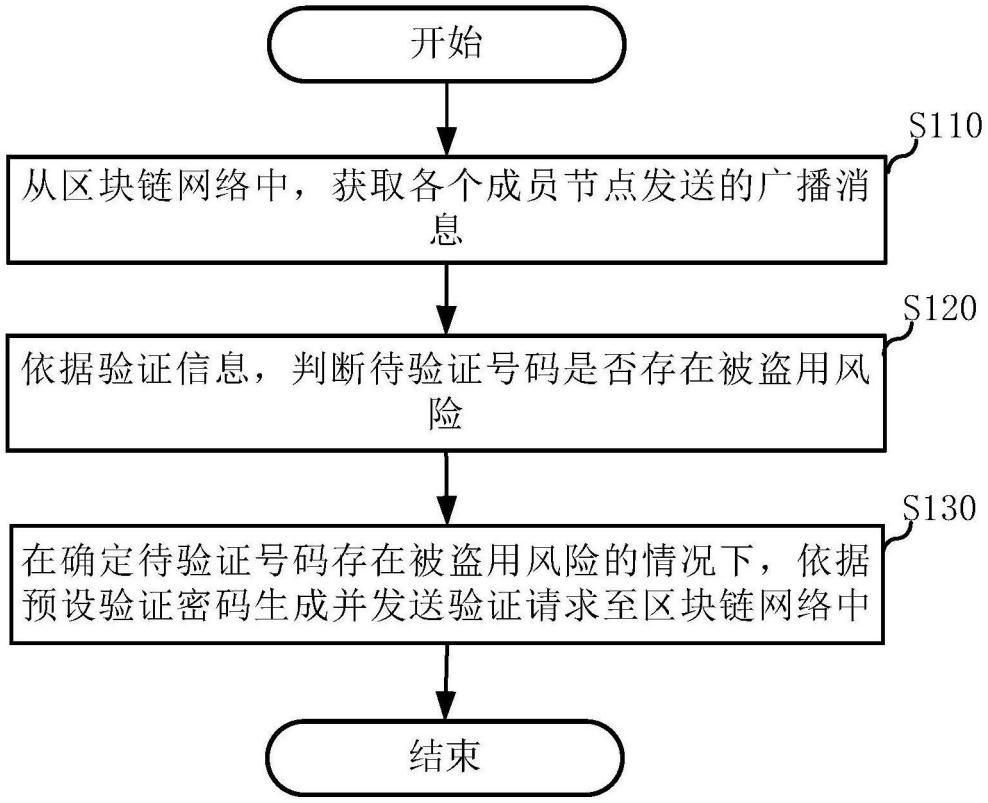

开始
S110
从区块链网络中，获取各个成员节点发送的广播消息
S120
依据验证信息，判断待验证号码是否存在被盗用风险
S130
在确定待验证号码存在被盗用风险的情况下，依据预设验证密码生成并发送验证请求至区块链网络中
结束

图1

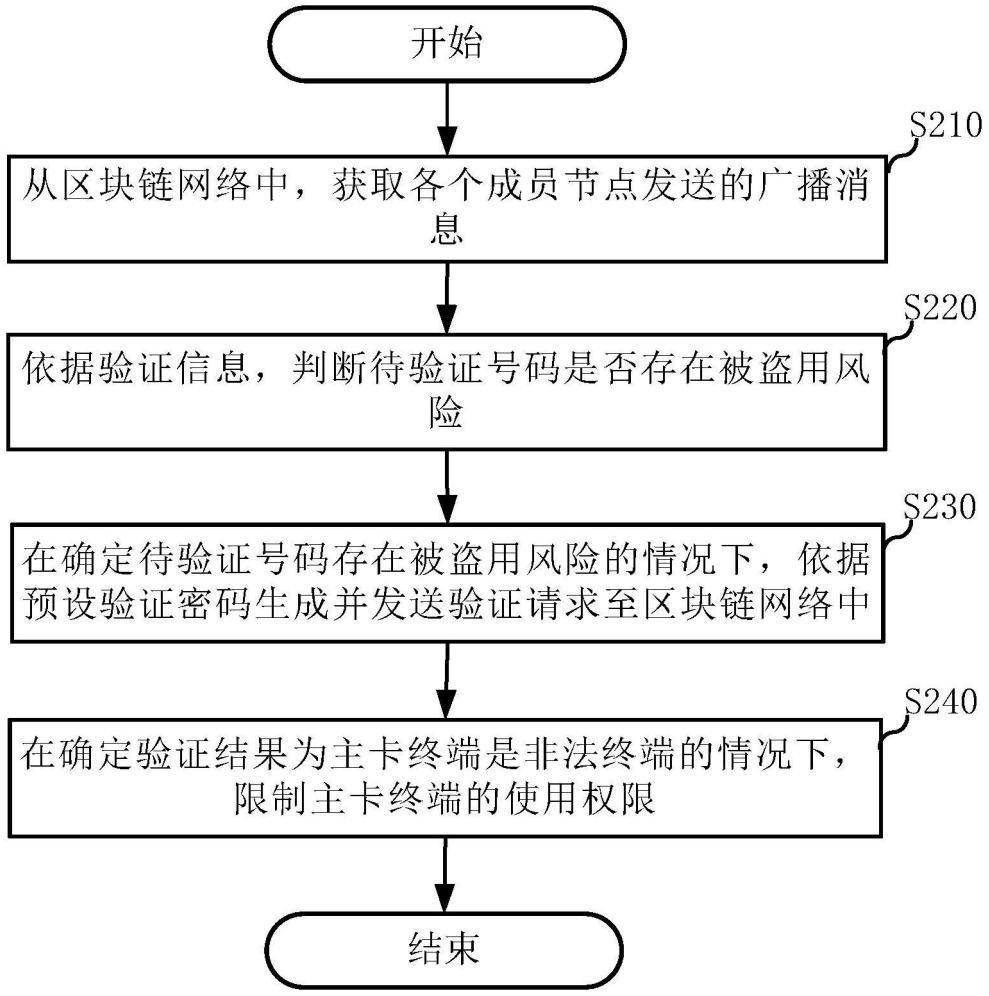

开始
S210
从区块链网络中，获取各个成员节点发送的广播消息
S220
依据验证信息，判断待验证号码是否存在被盗用风险
S230
在确定待验证号码存在被盗用风险的情况下，依据预设验证密码生成并发送验证请求至区块链网络中
S240
在确定验证结果为主卡终端是非法终端的情况下，限制主卡终端的使用权限
结束

图2

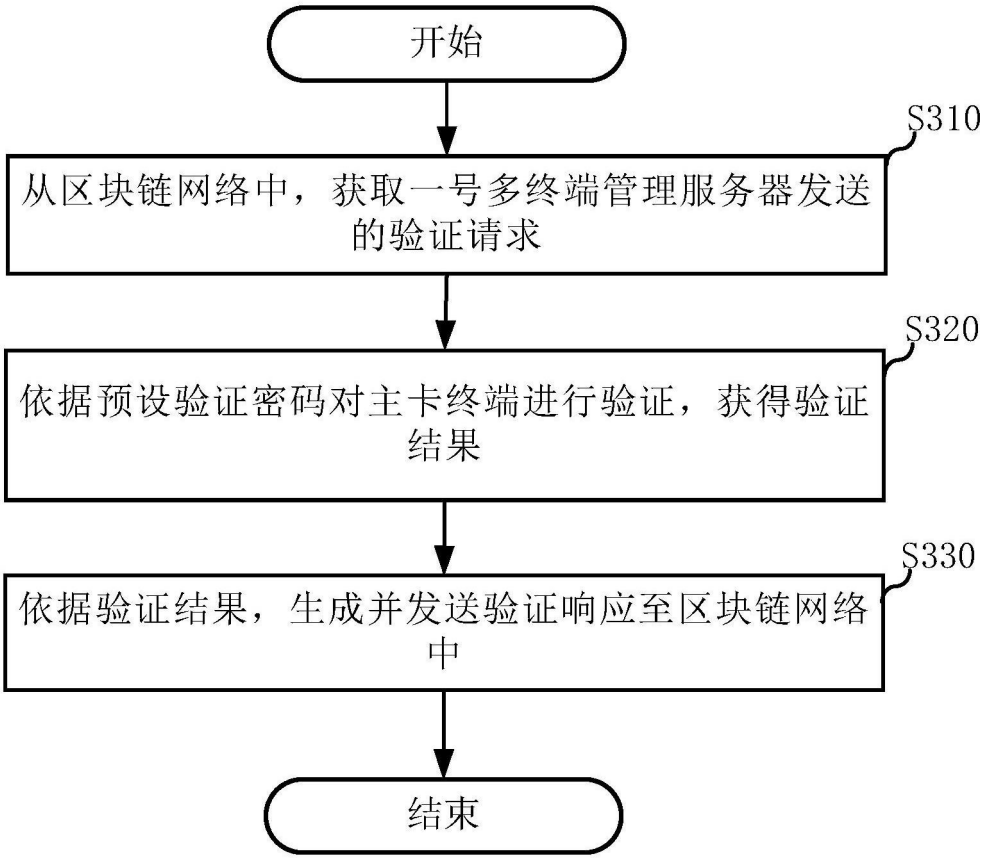

开始
S310
从区块链网络中，获取一号多终端管理服务器发送的验证请求
S320
依据预设验证密码对主卡终端进行验证，获得验证结果
S330
依据验证结果，生成并发送验证响应至区块链网络中
结束

图3


第一获取模块401
判断模块402
第一验证模块403

图4


第二获取模块501
第二验证模块502
处理模块503

图5

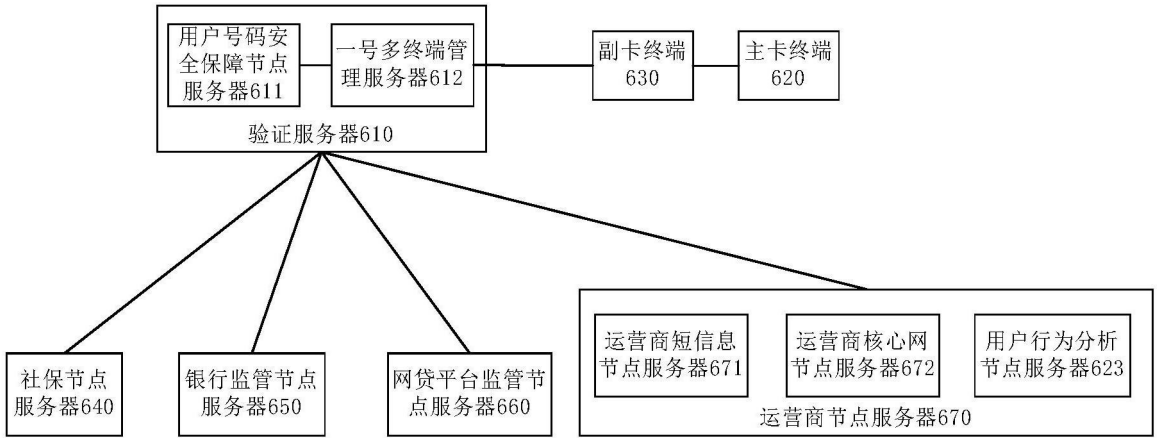

用户号码安全保障节点服务器611
一号多终端管理服务器612
副卡终端630
主卡终端620
验证服务器610
社保节点服务器640
银行监管节点服务器650
网贷平台监管节点服务器660
运营商短信息节点服务器671
运营商核心网节点服务器672
用户行为分析节点服务器623
运营商节点服务器670

图6

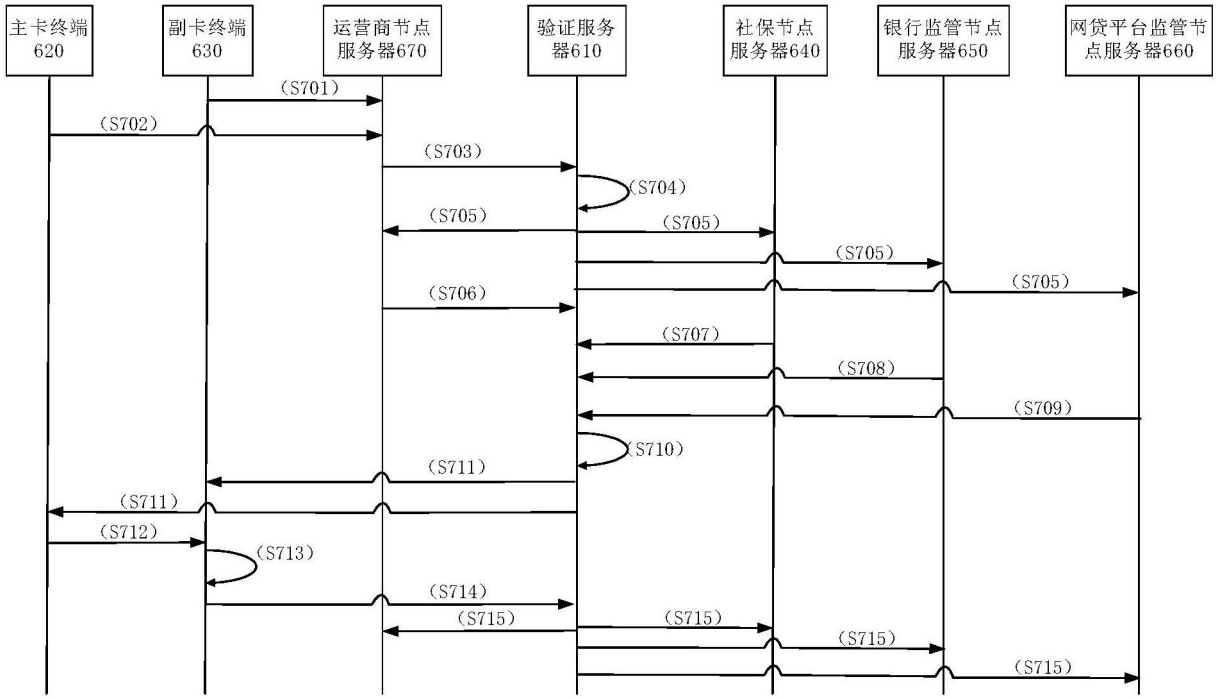

主卡终端620
副卡终端630
运营商节点服务器670
验证服务器610
社保节点服务器640
银行监管节点服务器650
网贷平台监管节点服务器660
(S701)
(S702)
(S703)
(S704)
(S705)
(S705)
(S705)
(S705)
(S706)
(S707)
(S708)
(S709)
(S710)
(S711)
(S711)
(S712)
(S713)
(S714)
(S715)
(S715)
(S715)
(S715)

图7