(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2020 年 9 月 17 日 (17.09.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/182005 A1

(51) 国际专利分类号:
G06Q 20/38 (2012.01)

(21) 国际申请号: PCT/CN2020/077388

(22) 国际申请日: 2020 年 3 月 2 日 (02.03.2020)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910177252.4 2019年3月8日 (08.03.2019) CN

(71) 申请人: 腾讯科技（深圳）有限公司 (TENCENT TECHNOLOGY (SHENZHEN) COMPANY LIMITED) [CN/CN]; 中国广东省深圳市南山区高新区科技中一路腾讯大厦35层, Guangdong 518057 (CN)。

(72) 发明人: 汪东艳(WANG, Dongyan); 中国广东省深圳市南山区高新区科技中一路腾讯大厦35层, Guangdong 518057 (CN)。 李茂材(LI, Maocai); 中国广东省深圳市南山区高新区科技中一路腾讯大厦35层, Guangdong 518057 (CN)。 李波(LI, Bo); 中国广东省深圳市南山区高新区科技中一路腾讯大厦35层, Guangdong 518057 (CN)。 屠海涛(TU, Haitao); 中国广东省深圳市南山区高新区科技中一路腾讯大厦35层, Guangdong 518057 (CN)。 王宗友(WANG, Zongyou); 中国广东省深圳市南山区高新区科技中一路腾讯大厦35层, Guangdong 518057 (CN)。

(74) 代理人: 深圳市深佳知识产权代理事务所（普通合伙）(SHENPAT INTELLECTUAL PROPERTY AGENCY); 中国广东省深圳市罗湖区南湖

(54) **Title:** METHOD FOR INFORMATION PROCESSING IN DIGITAL ASSET CERTIFICATE INHERITANCE TRANSFER, AND RELATED DEVICE

(54) **发明名称:** 数字资产凭证继承转移中的信息处理方法、和相关装置

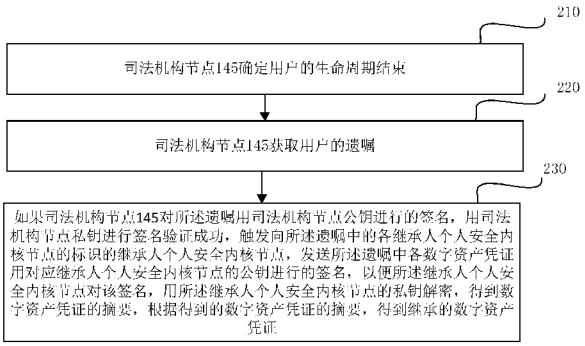

图 3

210 A judicial institution node 145 determines that the life cycle of a user has ended
220 The judicial institution node 145 acquires a will of the user
230 If signature verification, performed using a judicial institution node private key, of a signature made using a judicial institution node public key for the will is successful, the judicial institution node 145 triggers the sending, to an heir personal security kernel node of each heir personal security kernel node identifier in the will, of a signature made by each digital asset certificate in the will using a public key corresponding to the heir personal security kernel node, so that the heir personal security kernel node decrypts the signature using a private key of the heir personal security kernel node to obtain a digest of the digital asset certificate, and obtains an inherited digital asset certificate according to the digest of the obtained digital asset certificate

(57) **Abstract:** Disclosed are a method for information processing in digital asset certificate inheritance transfer, and a related device. The method comprises: determining that the life cycle of a user has ended (210); acquiring a will of the user (220); and if signature verification, performed using a judicial institution node private key, of a signature made using a judicial institution node public key for the will is successful, triggering the sending, to an heir personal security kernel node of each heir personal security kernel node identifier in the will, of a signature made by each digital asset certificate in the will using a public key corresponding to the heir personal

WO 2020/182005 A1

[见续页]

街道春风路庐山大厦B座18C2、18D、18E、18E2, Guangdong 518001 (CN)。

(81) 指定国(除另有指明，要求每一种可提供的国家保护)：AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(84) 指定国(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布：

— 包括国际检索报告(条约第21条(3))。

security kernel node, thereby realizing the unified maintenance of a digital asset certificate of a user.

(57) 摘要：一种数字资产凭证继承转移中的信息处理方法、和相关装置。该方法包括：确定用户的生命周期结束（210）；获取用户的遗嘱（220）；如果对所述遗嘱用司法机构节点公钥进行的签名，用司法机构节点私钥进行签名验证成功，触发向所述遗嘱中的各继承人个人安全内核节点的标识的继承人个人安全内核节点，发送所述遗嘱中各数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名，实现对用户的数字资产凭证进行统一的维护。

数字资产凭证继承转移中的信息处理方法、和相关装置

本申请要求于2019年03月08日提交中国专利局、申请号为201910177252.4、申请名称为“数字资产凭证继承转移中的信息处理方法、和相关装置”的中国专利申请，以及于2019年03月08日提交中国专利局、申请号为201910943397.0、申请名称为“数字资产凭证继承转移中的信息处理方法、和相关装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请涉及用户身份信息技术领域，具体涉及数字资产凭证继承转移中的信息处理技术。

背景技术

在现实生活中，资产转移往往是依据实物资产凭证进行。随着互联网的普及，越来越多的数字资产凭证以更快的速度在互联网上流转。例如，人们在购买理财产品时，由于实时性很高，交易所已经不再缺省提供实物凭证。资产的保存和转移往往需要登录不同的资产发行网站或者交易网站，个人用户难以对越来越多的数字资产凭证进行集中管理。而且，这些数字资产凭证很容易随着用户的生命周期结束（如离世）而丢失。例如，用户离世后，其资产不被人所知，导致继承人无法依法继承或者找回资产凭证。典型的例子是，因QuadrigaCX交易所创始人意外病故，导致价值约1.47亿美元的数字货币无法取出的事件。

现有技术中，缺少一种信息处理技术，能够对用户的数字资产凭证进行统一的管理。

发明内容

本申请提出一种信息处理技术，能够对用户的数字资产凭证进行统一的维护。

根据本申请实施例的一方面，公开了一种数字资产凭证继承转移中的信息处理方法，所述方法由司法机构节点执行，所述方法包括：

确定用户的生命周期结束；

获取用户的遗嘱，所述遗嘱包括用户个人安全内核节点的标识、各继承人个人安全内核节点的标识、各数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名、所述遗嘱用司法机构节点公钥进行的签名；

如果对所述遗嘱用司法机构节点公钥进行的签名，用司法机构节点私钥进行签名验证成功，触发向所述遗嘱中的各继承人个人安全内核节点的标识的继承人个人安全内核节点，发送所述遗嘱中各数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名，以便所述继承人个人安全内核节点对该签名，用所述继承人个人安全内核节点的私钥解密，得到数字资产凭证的摘要，根据得到的数字资产凭证的摘要，得到继承的数字资产凭证。

根据本申请实施例的一方面，公开了一种司法机构节点，包括：

生命周期结束确定单元，用于确定用户的生命周期结束；

遗嘱获取单元，用于获取用户的遗嘱，所述遗嘱包括用户个人安全内核节点的标识、各继承人个人安全内核节点的标识、各数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名、所述遗嘱用司法机构节点公钥进行的签名；

数字资产凭证签名发送单元，用于如果对所述遗嘱用司法机构节点公钥进行的签名，用司法机构节点私钥进行签名验证成功，触发向所述遗嘱中的各继承人个人安全内核节点的标识的继承人个人安全内核节点，发送所述遗嘱中各数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名，以便所述继承人个人安全内核节点对该签名，用所述继承人个人安全内核节点的私钥解密，得到数字资产凭证的摘要，根据得到的数字资产凭证的摘要，得到继承的数字资产凭证。

根据本申请实施例的一方面，公开了一种数字资产凭证继承转移中的信息处理方法，所述方法由司法机构节点执行，所述方法包括：

当用户的个人安全内核节点中增加数字资产凭证时，获取增加的数字资产凭证对应的继承人个人安全内核节点标识，以及所述继承人个人安全内核节点标识的继承人个人安全内核节点的公钥；

对增加的数字资产凭证，用所述继承人个人安全内核节点的公钥进行签名，得到增加的数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名；

将所述继承人个人安全内核节点标识、增加的数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名，添加到所述用户的遗嘱中，所述遗嘱中包含有用司法机构节点公钥进行的签名；

将所述遗嘱中包含的用司法机构节点公钥进行的签名去掉；

将所述遗嘱中的当前内容用所述司法机构节点公钥进行签名，并将得到的签名放入所述遗嘱。

根据本申请实施例的一方面，公开了一种司法机构节点，包括：

获取单元，用于当用户的个人安全内核节点中增加数字资产凭证时，获取增加的数字资产凭证对应的继承人个人安全内核节点标识，以及所述继承人个人安全内核节点标识的继承人个人安全内核节点的公钥；

第一签名处理单元，用于对增加的数字资产凭证，用所述继承人个人安全内核节点的公钥进行签名，得到增加的数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名；

添加单元，用于将所述继承人个人安全内核节点标识、增加的数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名，添加到所述用户的遗嘱中，所述遗嘱中包含有用司法机构节点公钥进行的签名；

第二签名处理单元，用于将所述遗嘱中包含的用司法机构节点公钥进行的签名去掉，将所述遗嘱中的当前内容用所述司法机构节点公钥进行签名，并将得到的签名放入所述遗嘱。

根据本申请实施例的一方面，公开了一种司法机构节点，包括：存储器，存储有计算机可读指令；处理器，读取存储器存储的计算机可读指令，以执行如上所述的方法。

根据本申请实施例的一方面，公开了一种计算机程序介质，其上存储有计算机可读指令，当所述计算机可读指令被计算机的处理器执行时，使计算机执行如上所述的方法。

根据本申请实施例的一方面，公开了一种包括指令的计算机程序产品，当其在计算机上运行时，使得所述计算机执行如上所述的方法。

本申请实施例中，用户的数字资产凭证维护在用户的个人安全内核节点中。继承人也有继承人个人安全内核节点，维护继承人的数字资产凭证。用户在生命周期期间会立有遗嘱，遗嘱中包括各继承人个人安全内核节点的标识，还有各数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名、所述遗嘱用司法机构节点公钥进行的签名。当司法机构节点确定用户生命周期结束后，获取用户的遗嘱，用自己的私钥对遗嘱中用司法机构节点公钥进行的签名进行验证。如果验证成功，说明自己就是用户生前指定执行继承首先的司法机构节点。然后，司法机构节点触发把遗嘱中各数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名发给相应继承人个人安全内核节点，只有真正的继承人个人安全内核节点采用继承人个人安全内核节点的私钥，能够解开该签名，获得继承的数字资产凭证。整个继承过程由机器自动执行，且由用司法机构节点公钥对遗嘱进行的签名来保证执行继承手续的第三方司法机构节点的可靠性，通过将数字资产凭证用继承人个人安全内核节点的公钥签名来保证只有真正的继承人才能解签名，保证继承过程中数字资产凭证的安全性，使得即使在用户生命周期结束时，相关的数字资产凭证仍然能自动安全转移到继承人。

本申请的其他特性和优点将通过下面的详细描述变得显然，或部分地通过本申请的实践而习得。

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的，并不能限制本申请。

附图说明

通过参照附图详细描述其示例实施例，本申请的上述和其它目标、特征及优点将变得更加显而易见。

图1A-B示出了根据本申请一个实施例的数字资产凭证继承转移中的信息处理方法应

用的系统构架图，其中，图1A是简略的系统构架图，图1B是在图1A的基础上对个人安全内核节点细化后的系统构架图。

图2A-K示出了根据本申请一个实施例的数字资产凭证继承转移中的信息处理方法应用在用户离世后数字资产凭证继承的应用场景下的界面图。

图3示出了根据本申请一个实施例的数字资产凭证继承转移中的信息处理方法的流程图。

图4示出了根据本申请一个实施例的验证遗嘱中用司法机构节点公钥对遗嘱进行的签名的具体流程图。

图5示出了根据本申请一个实施例的数字资产凭证继承转移中的信息处理方法的流程图。

图6示出了根据本申请一个实施例的遗嘱的生成过程流程图。

图7示出了根据本申请一个实施例的遗嘱的更新过程流程图。

图8示出了根据本申请一个实施例的遗嘱的更新过程流程图。

图9示出了根据本申请一个实施例的司法机构节点的框图。

图10示出了根据本申请一个实施例的司法机构节点的硬件图。

具体实施方式

现在将参考附图更全面地描述示例实施方式。然而，示例实施方式能够以多种形式实施，且不应被理解为限于在此阐述的范例；相反，提供这些示例实施方式使得本申请的描述将更加全面和完整，并将示例实施方式的构思全面地传达给本领域的技术人员。附图仅为本申请的示意性图解，并非一定是按比例绘制。图中相同的附图标记表示相同或类似的部分，因而将省略对它们的重复描述。

此外，所描述的特征、结构或特性可以以任何合适的方式结合在一个或更多示例实施方式中。在下面的描述中，提供许多具体细节从而给出对本申请的示例实施方式的充分理解。然而，本领域技术人员将意识到，可以实践本申请的技术方案而省略所述特定细节中的一个或更多，或者可以采用其它的方法、组元、步骤等。在其它情况下，不详细示出或描述公知结构、方法、实现或者操作以避免喧宾夺主而使得本申请的各方面变得模糊。

附图中所示的一些方框图是功能实体，不一定必须与物理或逻辑上独立的实体相对应。可以采用软件形式来实现这些功能实体，或在一个或多个硬件模块或集成电路中实现这些功能实体，或在不同网络和/或处理器装置和/或微控制器装置中实现这些功能实体。

下面先参照图1A-1B描述一下本申请实施例的数字资产凭证继承转移中的信息处理方法所应用的体系构架。

如图1A所示的体系构架包括个人安全内核节点107、依赖方节点109、依赖方资格证明方节点100、业务级用户身份凭证证明方节点104、法定用户身份凭证证明方节点105、社交操作系统级用户身份凭证证明方节点106、依赖方业务员终端108、司法机构节点145、调查节点146。上述所有节点都是区块链网络中的一个区块链节点，其在本申请实施例过程中产生的各种数据都可以记录到区块链，也可以从区块链获取数据。

个人安全内核节点 107 是一个保存用户的数字资产凭证的安全核心。每个用户有一个对应的个人安全内核节点 107。它是管理用户数字资产凭证的核心节点。数字资产凭证是以数字化存证形式存在的资产，如电子存储的理财产品。数字资产凭证往往是用户与依赖方节点 109 履行某一业务后依赖方节点 109 对用户负有的义务。例如，电子理财产品是在用户履行了购买后，作为理财公司的依赖方节点 109 对用户负有的支付利息和返还本金的义务的体现。

如图 1B 所示，个人安全内核节点 107 可以包括个人安全内核节点客户端 115 和个人安全内核节点服务器 116。个人安全内核节点客户端 115 是在用户终端上安装的、用于用户身份资产管理的客户端，个人安全内核节点服务器 116 是与个人安全内核节点客户端 115 配合进行用户身份资产管理的服务器。

依赖方节点 109 是指用户的业务履行所要依赖的一方的节点，一般是依赖的一方的服务器节点。例如，在购买理财产品业务中，用户要依赖理财公司来完成购买，理财公司的

服务器就是理财产品购买业务中的依赖方节点109。

依赖方业务员终端108是指依赖方与用户具体业务履行时进行业务履行操作的业务员所用的终端。例如，在理财产品购买业务中，具体与用户进行理财产品购买对接的柜台人员用的终端就是依赖方业务员终端108。法定用户身份凭证证明方节点105是用户法定身份注册的节点，而且法定用户身份凭证证明方节点105用于在业务履行前证明用户的身份合法，使得在用户的身份被证明合法之后，用户才能履行业务，从而获得与依赖方节点履行业务产生的数字资产凭证。业务级用户身份凭证证明方节点104是指曾经与用户履行过业务的平台服务器。因该平台曾经与用户履行过业务，对用户的身份进行过验证，使得在对身份认证确信等级要求不太高的情况下，这样的平台可以起到一个间接验证用户身份的作用。社交操作系统级用户身份凭证证明方节点106是为用户提供身份证明的社交操作系统级平台服务器。这些平台具备较强的数据安全保护能力，并具备普遍服务能力，例如微信平台服务器、Facebook平台服务器。可以认为这样的业务提供方提供了一个行业内普遍使用的社交操作系统，鉴于这类操作系统级的身份鉴别不仅仅是以某个中心化预先发行的静态法定身份凭证为身份核验的依据，而是结合采用了多维的基于社交圈以及用户活动状态确认的非中心化身份核验体系，以避免中心化发行的静态身份核验组件丢失后的身份冒用风险。所以在业务履行前对用户身份的核验确信等级更高，社交操作系统用于身份核验的确信等级评价与社交操作系统承载的用户数目，应用（例如小程序应用）和内容等相关。由于该部分不是本申请重点关注的内容，不在此详述。依赖方资格证明方节点100是指对依赖方是否有权限要求用户提供用户身份凭证的资格进行认证的终端。在业务履行前，用户的身份需要经法定用户身份凭证证明方节点105，或业务级用户身份凭证证明方节点104，或社交操作系统级用户身份凭证证明方节点106证明，而依赖方资格需要经依赖方资格证明方节点100确定。它们都是履行业务从而形成电子理财产品等数字资产凭证之前用到的节点，与本申请实施例不直接相关，故不赘述。

司法机构节点145是司法机构（例如法院）用来对遗嘱进行执行处理的终端，例如法院处理遗嘱业务的服务器。

调查节点146是司法机构（例如法院）委托的调查继承中的信息的单位的处理终端，如法院的调查委员会的终端。

下面结合图2A至图2K描述根据本申请实施例的数字资产凭证继承转移中的信息处理方法应用在用户离世后数字资产凭证继承应用场景下的界面图。

图2A示出了个人安全内核节点（Persk）107关联的用户终端显示的功能选择界面图。如前所述，个人安全内核节点107是维护用户的数字资产凭证的设备，可以体现为用户终端中的一个客户端，或用户终端的一个芯片，或植入人体或贴在皮肤表面的金属贴片、芯片或者其他具备存储和计算能力的单元。当个人安全内核节点107为用户终端中的一个客户端，或用户终端的一个芯片或者其他具备存储和计算能力的单元时，个人安全内核节点107关联的用户终端是指安装有显示屏的用户终端。当个人安全内核节点107为植入人体或贴在皮肤表面的金属贴片、芯片或者其他具备存储和计算能力的单元时，个人安全内核节点107关联的用户终端是指与该金属贴片、芯片或者其他具备存储和计算能力的单元通信并显示其中存储的数字资产凭证的终端。

当用户的生命周期未结束之前，用户可以在图2A所示的界面选择“设立遗嘱”功能选项，进入如图2B所示的界面。

在图2B的界面上，罗列了用户的所有数字资产凭证或者各种数字资产凭证类型，让用户去填写用户希望其每一项数字资产凭证或者每一数字资产凭证类型的继承人，并填写执行遗嘱的司法机构。执行遗嘱的司法机构的作用是启动并见证该数字资产凭证在用户生命周期结束后向指定的继承人转移的过程，起到公信的作用。

当用户在图2B的界面上针对每一项数字资产凭证填写完继承人和见证的司法机构后，如图2C所示，开始获取继承人、指定的司法机构的公钥。继承人的公钥是为了保证用户生命周期结束后给继承人的数字资产凭证的安全性。司法机构的公钥是为了对执行遗嘱的第三方司法机构是否是用户真正想要的司法机构进行验证，提高遗嘱的保密性。由于用户的

遗嘱用司法机构的公钥进行签名，只有真正的司法机构，才能解签名，通过验证，进行后续程序。

获得继承人的公钥后，用继承人的公钥对其对应的数字资产凭证进行签名。将用户Persk标识、继承人Persk标识、用继承人的公钥对数字资产凭证进行的签名放到遗嘱中。获得司法机构的公钥后，用司法机构公钥对当前遗嘱内容进行签名，将该签名也放入遗嘱中。此时遗嘱的内容如图2D所示，包括用户Persk标识、继承人Persk标识、用各继承人的公钥对相应数字资产凭证进行的签名、用司法机构公钥生成的遗嘱签名。各继承人的公钥对相应数字资产凭证进行的签名只有继承人自己用私钥才能解开，保证继承中数字资产凭证传递的安全性。用司法机构公钥生成的遗嘱签名只有用用户指定的司法机构的私钥才能通过验证，保证继承过程的可信性。

然后，如图2E所示，将生成的遗嘱记录到区块链上。

图2F-K不再是用户终端的界面图，而是司法机构节点145的界面图。用户在离世之前，在加入区块链网络时与区块链网络运营商签立智能合约。图1A-B的每个节点都作为一个区块链网络节点，能够获取到该智能合约。该智能合约中，用户指定离世后的继承程序发起人、证明人。

当接收到用户A的亲友B发出的、对用户A已经离世的启动请求时，显示图2F所示的界面。如果B恰恰是用户智能合约中指定的继承程序发起人，则开始继承验证程序，即将智能合约中指定的证明人C、D、E发出用户A离世确认请求，要求确认用户A是否真的离世，如图2G所示。

如果从证明人C、D、E都接到用户A已经离世的应答，确定用户A离世，开始继承程序，如图2H所示。

当司法机构节点145的工作人员在图2H的界面上选择“确认”后，进入图2I所示的界面，从区块链上找到带有用户A的Persk标识的遗嘱。由于区块链上的遗嘱包括用户Persk标识、继承人Persk标识、用各继承人的公钥对相应数字资产凭证进行的签名、用司法机构公钥生成的遗嘱签名，因此可以找到该遗嘱。然后，司法机构对遗嘱中的用司法机构公钥生成的遗嘱进行签名验证，如图2J所示。

如果签名验证成功，将遗嘱中用各继承人的公钥对相应数字资产凭证进行的签名取出，向遗嘱中对应继承人Persk标识的Persk发送，如图2K所示。继承人Persk收到后，用继承人私钥解签名，得到数字资产凭证的摘要，凭该摘要获得数字资产凭证。如果不是真正的继承人，没有继承人私钥，无法用该私钥解签名，也就得不到继承的数字资产凭证。

上述只是围绕用户离世后的数字资产凭证继承的应用场景展开描述，在用户失踪等其他应用场景中过程类似。

根据本申请的一个实施例，提供了一种数字资产凭证继承转移中的信息处理方法。数字资产凭证是以数字化形式存在的资产凭证，如电子理财产品单。数字资产凭证继承转移是指用户生命周期结束后用户的数字资产凭证转移到对应的继承人。生命周期是指用户从出生到离世或宣告失踪的期间，生命周期结束包括离世和宣告失踪。

另外，本申请提供的数字资产凭证继承转移中的信息处理方法由司法机构节点145执行，而且如图3所示，所述方法包括：

步骤210、司法机构节点145确定用户的生命周期结束；

步骤220、司法机构节点145获取用户的遗嘱，所述遗嘱包括用户个人安全内核节点的标识、各继承人个人安全内核节点的标识、各数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名、所述遗嘱用司法机构节点公钥进行的签名；

步骤230、如果司法机构节点145对所述遗嘱用司法机构节点公钥进行的签名，用司法机构节点私钥进行签名验证成功，触发向所述遗嘱中的各继承人个人安全内核节点的标识的继承人个人安全内核节点，发送所述遗嘱中各数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名，以便所述继承人个人安全内核节点对该签名，用所述继承人个人安全内核节点的私钥解密，得到数字资产凭证的摘要，根据得到的数字资产凭证的摘要，得到继承的数字资产凭证。

下面对以上步骤详细描述。

在步骤 210，司法机构节点 145 确定用户的生命周期结束。

确定用户的生命周期结束可以采取官方发起的方式，也可以采用民间发起的方式，也可以采用官方和民间共同确认的方式。

在官方发起的方式中，步骤 210 包括：

司法机构节点 145 响应于来自调查节点 146 的生命周期结束通知，确定用户的生命周期结束。

调查节点 146 是司法机构委托的调查遗嘱继承中的各种情况的机构的终端。例如，司法机构是法院的情况下，调查节点 146 是法院设立的调查委员会的终端。当有人在法院报案用户离世或失踪后，法院委托调查委员会的人员调查该用户的社交关系，作出用户是否真正离世或应当被宣告失踪的判断，在调查节点 146 由该人员根据该判断结果生成生命周期结束通知，发送给司法机构节点 145。生命周期结束通知是宣告用户已经离世或宣告失踪的消息。

该实施例的好处是，生命周期结束通知是由调查节点 146 的相关人员实际调查情况后得到的，比较全面，误差小。

在民间发起的方式中，步骤 210 包括：

司法机构节点 145 接收到启动节点的启动请求；

司法机构节点 145 通过社交操作系统平台，向多个证明方节点发送用户生命周期结束确认消息；

如果所述多个证明方节点的应答满足预定条件，则司法机构节点 145 确定用户的个人安全内核节点的生命周期结束。

启动节点是对遗嘱继承程序进行启动的终端。

在一个实施例中，启动节点用户是任何终端（包括法院终端等），即只要有人启动，就开启继承过程。

在另一个实施例中，启动节点是用户通讯录中的用户终端。也就是说，只有用户认识的人才能开启继承程序，避免假报案和无关骚扰。由于用户离世或失踪后，其个人安全内核节点客户端很可能也找不到，但用户的通讯录可以存储在个人安全内核节点服务器，从个人安全内核节点服务器中可以获取用户通讯录。

在另一个实施例中，启动节点是用户在生命周期期间在智能合约中指定的启动节点。例如，用户在生命周期期间，可以在智能合约指定一个启动节点标识，如某朋友的终端标识。该智能合约可以与用户个人安全内核节点标识对应，保存在所有区块链节点，也可以保存在区块链上。启动请求中含有用户个人安全内核节点标识，司法机构节点 145 可以从该启动请求中获得用户个人安全内核节点标识，从本地或者区块链上找到与该用户个人安全内核节点标识对应的智能合约，从而获取其中的启动节点标识。如果该标识是启动请求的发出者的标识，则开启继承过程。该实施例提高了开启继承的安全性。

在一个实施例中，智能合约是通过如下过程生成的：

显示智能合约模板列表；

响应于用户从智能合约模板列表选择智能合约模板并在选择的智能合约模板中填写内容，将填写的内容整合到智能合约模板中，为用户生成智能合约。

也就是说，系统内为用户提供多种智能合约模板，在模板中有一部分用户需要填写的内容。用户可以通过例如勾选的方式在列表中选择一个智能合约模板，并在模板中需要填写内容的位置填写内容。将用户填写的内容整合到选择的智能合约模板中，生成智能合约。

社交操作系统平台是指为用户提供身份证明、比一般应用服务完全平台具备更强的数据安全保护能力和普遍服务能力的平台，例如微信平台服务器、Facebook 平台服务器。由于在该平台注册了大量用户，因此，可以通过该平台向多个证明方节点发送继承程序启动确认请求消息。继承程序启动确认请求是指要求确认用户是否离世或失踪，以便决定是否开启继承程序的请求。

在一个实施例中，所述多个证明方节点从用户通讯录中随机选出。用户通讯录如上所

述，可以从个人安全内核节点服务器中获取。该实施例中好处是，由于通讯录都是用户认识的人，从中随机选出，避免用户勾结一些好友作弊的风险。

在一个实施例中，所述多个证明方节点标识由用户在用户生命周期期间指定，并与上述启动节点一样，记录在智能合约中。智能合约与用户个人安全内核节点标识对应，存储在每个区块链节点上，或者存储在区块链上。司法机构节点 145 从启动请求中获得用户个人安全内核节点标识，在本地或区块链上查找到对应的智能合约，从智能合约中找到多个证明方节点标识，通过社交操作系统平台，向多个证明方节点发送用户生命周期结束确认消息。该实施例提高了用户选择遗嘱执行过程的灵活性。

这里的预定条件是指预先设定、多个证明方节点的应答应满足的条件。在一个实施例中，预定条件是，所述多个证明方节点的应答都是确认用户生命周期结束的应答。在一个实施例中，预定条件是，所述多个证明方节点中预定比例以上的应答都是确认用户生命周期结束的应答。

该民间发起的方式的优点是自动通过机器节点执行，自动化程度高，且避免政府审批调查的冗长耗时。

在官方和民间共同确认的方式中，所述如果所述多个证明方节点的应答满足预定条件，则司法机构节点 145 确定用户的生命周期结束，包括：

如果所述多个证明方节点的应答满足预定条件，且接收到来自调查节点的生命周期结束通知，则司法机构节点 145 确定用户的个人安全内核节点的生命周期结束。

也就是说，仅多个证明方节点的应答满足预定条件是不够的，还需要官方也给出了生命周期结束通知，两个条件都满足，才能确定用户的生命周期结束。该实施例提高了确定用户的生命周期结束的安全性。

在步骤 220 中，司法机构节点 145 获取用户的遗嘱，所述遗嘱包括用户个人安全内核节点的标识、各继承人个人安全内核节点的标识、各数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名、所述遗嘱用司法机构节点公钥进行的签名。

在一个实施例中，司法机构节点 145 获取用户的遗嘱包括：司法机构节点 145 获取与用户的个人安全内核节点的标识对应的用户的遗嘱。也就是说，司法机构节点 145 可以按照用户的个人安全内核节点的标识，获取对应的用户的遗嘱。

用户个人安全内核节点的标识是将用户个人安全内核节点区别于其它人的个人安全内核节点的标记，它可以由字母、数字、符号等及其组合表示。遗嘱中记录用户个人安全内核节点的标识，是为了当用户生命周期结束后，根据该标识找到对应的遗嘱（包含该标识的遗嘱）。

各继承人个人安全内核节点的标识是针对用户的数字资产凭证，用户指定继承的人的个人安全内核节点的标识，是将该继承人个人安全内核节点区别于其它人的个人安全内核节点的标记。遗嘱中，针对每一项数字资产凭证，可以有不同的继承人个人安全内核节点的标识。

各数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名是指，针对用户的各数字资产凭证，根据预定摘要算法生成摘要，用对应继承人个人安全内核节点的公钥对摘要加密得到的结果。直接传递数字资产凭证，被第三方截获，可以从中方便地取走数字资产凭证。由于签名是先生成摘要，再由对应继承人个人安全内核节点的公钥加密得到的，没有继承人个人安全内核节点的公钥是无法解签名的，提高了继承中数字资产凭证转移的安全性。

所述遗嘱用司法机构节点公钥进行的签名，是指用司法机构节点公钥对遗嘱当前内容进行的签名，包括对遗嘱当前内容按照预定摘要算法生成摘要、和用司法机构节点公钥对摘要加密。它具有验证执行遗嘱的司法机构节点是否是用户指定的司法机构节点的作用，因为如果执行遗嘱的司法机构节点不是用户指定的司法机构节点，它不具有司法机构节点私钥，无法对签名验证成功。它保证了继承中司法机构节点的可信度，提高继承程序的安全性。

在遗嘱生成之后，可以记录到区块链上，也可以存储在用户的个人安全内核节点服务

器。这是因为，用户生命周期结束后，很可能个人安全内核节点客户端也随着用户终端的丢失而丢失，遗嘱也可能消亡，将其存储在区块链上或个人安全内核节点服务器上，可以在用户生命周期结束后找回遗嘱。

在遗嘱上链存储的实施例中，步骤 220 包括：司法机构节点 145 从区块链上获取含有用户的个人安全内核节点的标识的遗嘱，作为与用户的个人安全内核节点的标识对应的用户的遗嘱，其中所述遗嘱生成后记录到该区块链上。

如上所述，所述遗嘱包括用户个人安全内核节点的标识、各继承人个人安全内核节点的标识、各数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名、所述遗嘱用司法机构节点公钥进行的签名。由于启动请求中包含用户个人安全内核节点的标识，司法机构节点可以查找区块链上包含该标识的遗嘱，该遗嘱就是与用户的个人安全内核节点的标识对应的用户的遗嘱。

在一个实施例中，遗嘱还包括头信息。该头信息中包含遗嘱特征字和遗嘱长度。从区块链上获取含有用户的个人安全内核节点的标识的遗嘱，包括：

在区块链中识别到带有遗嘱特征字的头信息之后，按照头信息中的遗嘱长度识别遗嘱所关联的数据区块；

在识别出的数据区块中，确定是否含有用户的个人安全内核节点的标识，如含有，则识别出的数据区块构成含有用户的个人安全内核节点的标识的遗嘱。

头信息是指遗嘱作为数据区块记录到区块链上后，每个数据区块的区块头信息。每个数据区块还有区块体，其中记录遗嘱中的内容。遗嘱可能包括多个数据区块。如上所述，遗嘱包括用户个人安全内核节点的标识、各继承人个人安全内核节点的标识、各数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名、所述遗嘱用司法机构节点公钥进行的签名，其中，不同继承人个人安全内核节点的标识、和相应不同的数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名可能记载在不同数据区块中。

遗嘱特征字是表示区块链上的数据区块是关于遗嘱的数据区块的标志。没有该遗嘱特征字，代表该数据区块记录的不是遗嘱。有该遗嘱特征字，代表该数据区块记录的是遗嘱。由于区块链上记录各种数据区块，有一些数据区块与遗嘱完全无关，为了缩小搜索范围，在存放遗嘱的数据区块的区块头中设置遗嘱特征字。在区块链上找到该遗嘱特征字，认为包含该遗嘱特征字的数据区块是遗嘱数据区块。

遗嘱长度是表明遗嘱占用了区块链上连续数据区块的数量的标志。例如，遗嘱长度为 7，代表在区块链上，从当前数据区块开始数 7 个数据区块，这些数据区块都是遗嘱关联的数据区块。

因此，在区块链中识别到带有遗嘱特征字的头信息之后，可以按照头信息中的遗嘱长度识别遗嘱所关联的数据区块，然后在这些数据区块范围内确定是否含有用户的个人安全内核节点的标识。这样做的好处是，相比于在整个区块链上搜索含有用户的个人安全内核节点的标识的数据区块，大大减小了搜索范围，提高了搜索效率。

如果确定在这些连续的数据区块范围内含有用户的个人安全内核节点的标识，该连续的数据区块范围（该遗嘱长度指示的数量的连续数据区块）构成含有用户的个人安全内核节点的标识的遗嘱。

在遗嘱存储在个人安全内核节点服务器的实施例中，所述个人安全内核节点包括个人安全内核节点客户端和个人安全内核节点服务器。步骤 220 包括：司法机构节点 145 从用户的个人安全内核节点的标识对应的个人安全内核节点服务器，获取遗嘱，作为与用户的个人安全内核节点的标识对应的用户的遗嘱，其中所述遗嘱由个人安全内核节点客户端生成后存储在个人安全内核节点服务器。

个人安全内核节点客户端生成遗嘱后，将其存储在个人安全内核节点服务器，该个人安全内核节点客户端和个人安全内核节点服务器具有同一个人安全内核节点标识。在启动请求中含有用户的个人安全内核节点的标识。这样，可以找到与该标识对应的个人安全内核节点服务器，从其获得遗嘱。

在步骤 230 中，如果司法机构节点 145 对所述遗嘱用司法机构节点公钥进行的签名，

用司法机构节点私钥进行签名验证成功，触发向所述遗嘱中的各继承人个人安全内核节点的标识的继承人个人安全内核节点，发送所述遗嘱中各数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名，以便所述继承人个人安全内核节点对该签名，用所述继承人个人安全内核节点的私钥解密，得到数字资产凭证的摘要，根据得到的数字资产凭证的摘要，得到继承的数字资产凭证。

司法机构节点 145 获取到遗嘱后，司法机构节点 145 不应立即开始执行继承过程。因为如果自己并不是用户指定的司法机构节点，则自己无权执行后续的继承程序的。因此，司法机构节点 145 要先对所述遗嘱用司法机构节点公钥进行的签名，用司法机构节点私钥进行签名验证。

在一个实施例中，所述遗嘱还包括指定的执行该遗嘱的司法机构节点标识。如图 2B 所示，用户在界面上指定执行该遗嘱的司法机构节点标识，从而在图 2D 的遗嘱中含有该标识。

在该实施例中，如图 4 所示，所述司法机构节点 145 对所述遗嘱用司法机构节点公钥进行的签名，用司法机构节点私钥进行签名验证成功，包括：

步骤 310、司法机构节点 145 获取遗嘱中指定的执行该遗嘱的司法机构节点标识；

步骤 320、如果遗嘱中指定的执行该遗嘱的司法机构节点标识是当前执行所述方法的司法机构节点的标识，司法机构节点 145 对所述遗嘱用司法机构节点公钥进行的签名，用司法机构节点私钥进行签名验证成功。

由于遗嘱中具有指定的执行该遗嘱的司法机构节点标识，因此，可以从遗嘱中获取该标识。由于司法机构节点 145 本地存储着自己的标识，司法机构节点 145 将获取的标识与本地存储的自己的标识进行比对，如果一致，则用司法机构节点私钥，对遗嘱中的所述遗嘱用司法机构节点公钥进行的签名进行验证。

该实施例的好处是，综合司法机构节点标识比较和用司法机构节点公钥生成的签名的验证两项，来进行司法机构节点的权限验证，比单纯检验签名，更能提高司法机构节点权限验证的准确性。

在一个实施例中，步骤 320 包括：

如果遗嘱中指定的执行该遗嘱的司法机构节点标识是当前执行所述方法的司法机构节点的标识，司法机构节点 145 对所述遗嘱用司法机构节点公钥进行的签名，用司法机构节点私钥解密，得到解密后产生的遗嘱摘要；

司法机构节点 145 生成所述遗嘱的摘要；

如果解密后产生的遗嘱摘要与生成的遗嘱的摘要一致，则司法机构节点 145 确定对所述遗嘱用司法机构节点公钥进行的签名，用司法机构节点私钥进行签名验证成功。

由于生成遗嘱签名是包括对遗嘱内容按照预定摘要算法（例如哈希算法）生成摘要、和对摘要用司法机构节点公钥加密的过程，验证签名时遵循相反的过程。首先用司法机构节点私钥对签名解密，得到遗嘱内容的摘要。然后，再按照生成签名时同样的摘要算法，生成所述遗嘱的摘要。由于在生成遗嘱签名时，遗嘱中还没有放入签名，生成遗嘱签名基于的是遗嘱中除遗嘱签名之外的内容，因此，在一个实施例中，生成所述遗嘱的摘要包括：

将遗嘱中的所述遗嘱用司法机构节点公钥进行的签名去除；

对去除所述签名后的遗嘱应用生成所述遗嘱时同样的预定摘要算法，生成遗嘱的摘要。

也就是说，它要遵循生成遗嘱的签名时对生成摘要相同的过程，先将遗嘱中的所述遗嘱用司法机构节点公钥进行的签名去除，因为在生成遗嘱的签名时并没有对包含该签名的遗嘱生成摘要再加密，而是在没有包含该签名之前对遗嘱的内容生成摘要然后加密。另外，在司法机构节点 145 还要保存与用户的个人安全内核节点中同样的预定摘要算法。这样，对去除所述签名后的遗嘱应用该预定摘要算法，生成的摘要与生成遗嘱签名时的摘要才具有一致的比对基础。

对去除所述签名后的遗嘱应用该预定摘要算法后，将解密后产生的遗嘱摘要与生成的遗嘱的摘要比对，如果二者一致，则签名验证成功，认为当前执行遗嘱的司法机构节点就

是用户指定的司法机构节点。这时，就可以触发向所述遗嘱中的各继承人个人安全内核节点的标识的继承人个人安全内核节点，发送所述遗嘱中各数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名。

触发的含义是可以由司法机构节点 145 自己完成，也可以指定另一其它节点完成，也可以启动区块链网络中的智能合约，由智能合约自动分配节点完成。

上述过程中，发送的是各数字资产凭证的签名而不是数字资产凭证本身，是因为第三方节点即使截获，也没有继承人个人安全内核节点的私钥，无法解签名，因而无法获得继承的数字资产凭证，提高继承中数字资产凭证的安全性。

由于对数字资产凭证用继承人个人安全内核节点的公钥签名包含对数字资产凭证根据预定摘要算法生成摘要，并对摘要用继承人个人安全内核节点的公钥加密的过程，解签名的过程也分为两步。首先，继承人个人安全内核节点对该签名，用所述继承人个人安全内核节点的私钥解密，得到数字资产凭证的摘要。然后，根据得到的数字资产凭证的摘要，得到继承的数字资产凭证。

根据得到的数字资产凭证的摘要，得到继承的数字资产凭证有多种实施方式。

在一个实施例中，所述根据得到的数字资产凭证的摘要，得到继承的数字资产凭证，包括：从区块链上获取与得到的数字资产凭证的摘要对应的数字资产凭证，其中，数字资产凭证生成后，与该数字资产凭证的摘要对应存储在区块链上。

该实施例遵循着数字资产凭证生成后立即上链的模式。用户个人安全内核节点与业务依赖方节点（例如理财公司终端）履行业务（例如签订购买理财产品的合同）后，生成与业务依赖方节点之间的数字资产凭证（例如理财产品单）。生成数字资产凭证后，立即根据预定摘要算法，生成该数字资产凭证的摘要，将该摘要与该数字资产凭证对应存储在区块链上。这样，从区块链上可以直接查询到得到的数字资产凭证的摘要对应的数字资产凭证。

在一个实施例中，个人安全内核节点包括个人安全内核节点客户端、和个人安全内核节点服务器。所述根据得到的数字资产凭证的摘要，得到继承的数字资产凭证，包括：从个人安全内核节点服务器获取与得到的数字资产凭证的摘要对应的数字资产凭证，其中，数字资产凭证由个人安全内核节点客户端生成后，与该数字资产凭证的摘要对应存储在个人安全内核节点服务器上。

该实施例中，个人安全内核节点客户端与业务依赖方节点生成数字资产凭证后，根据预定摘要算法，生成该数字资产凭证的摘要，将该摘要与该数字资产凭证对应存储在个人安全内核节点服务器上。这样，从个人安全内核节点服务器可以直接查询到得到的数字资产凭证的摘要对应的数字资产凭证。

在一个实施例中，所述遗嘱中还包括各数字资产凭证的业务依赖方节点标识。所述触发向所述遗嘱中的各继承人个人安全内核节点的标识的继承人个人安全内核节点，发送所述遗嘱中各数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名，包括：触发向所述遗嘱中的各继承人个人安全内核节点的标识的继承人个人安全内核节点，发送所述遗嘱中各数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名、以及各数字资产凭证的业务依赖方节点标识。

此时，所述根据得到的数字资产凭证的摘要，得到继承的数字资产凭证，包括：

向数字资产凭证的业务依赖方节点标识的业务依赖方节点发送得到的数字资产凭证的摘要；

从所述业务依赖方节点接收与所述数字资产凭证的摘要对应的数字资产凭证。

数字资产凭证都是用户个人安全内核节点与一个业务依赖方节点履行业务形成的，形成数字资产凭证后该数字资产凭证和该数字资产凭证的摘要在该业务依赖方节点备份保存。因此，可以从该业务依赖方节点，凭数据资产凭证的摘要，调回相应数字资产凭证。为了向业务依赖方节点请求，遗嘱中要包含该业务依赖方节点的标识，它可以在生成遗嘱时根据数字资产凭证中含有的业务依赖方节点标识生成（业务依赖方节点标识是数字资产凭证的重要字段，没有该字段无法兑现该数字资产）。向继承人个人安全内核节点发送数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名时，将该业务依赖方节点标识

也同时发送。这样，继承人个人安全内核节点就可以向数字资产凭证的业务依赖方节点标识的业务依赖方节点发送得到的数字资产凭证的摘要。在业务依赖方节点，数字资产凭证与其摘要对应存储，这样，从所述业务依赖方节点就可以接收到与所述数字资产凭证的摘要对应的数字资产凭证。

在一个实施例中，所述继承的数字资产凭证中包含数字资产凭证依赖的业务依赖方节点标识，以便所述继承人个人安全内核节点与该业务依赖方节点标识的业务依赖方节点，根据继承的数字资产凭证，生成继承人节点与该业务依赖方节点之间的更新后数字资产凭证。

也就是说，虽然在步骤 230 中，继承人个人安全内核节点得到了继承的数字资产凭证，但该数字资产凭证仅是用户个人安全内核节点与依赖方节点形成的，并非继承人个人安全内核节点与依赖方节点形成的，因此，继承人个人安全内核节点要与依赖方节点形成更新后数字资产凭证。

在一个实施例中，所述与该业务依赖方节点标识的业务依赖方节点，根据继承的数字资产凭证，生成继承人节点与该业务依赖方节点之间的更新后数字资产凭证包括由继承人个人安全内核节点执行的以下过程：

继承人个人安全内核节点向该业务依赖方节点标识的业务依赖方节点，发送继承的数字资产凭证和继承人个人安全内核节点标识，以便所述业务依赖方节点根据继承的数字资产凭证和继承人个人安全内核节点标识，生成更新后数字资产凭证；

继承人个人安全内核节点接收所述业务依赖方节点发送的更新后数字资产凭证。

由于更新后数字资产凭证中的依赖方节点义务与继承的数字资产凭证的依赖方节点义务完全一致，只不过当事人由用户个人安全内核节点和业务依赖方节点分别变成了继承人个人安全内核节点和业务依赖方节点，因此，可以将继承数字资产凭证内容中仅将当事人信息由用户个人安全内核节点标识和业务依赖方节点标识分别变成继承人个人安全内核节点标识和业务依赖方节点标识，得到更新后数字资产凭证，向继承人个人安全内核节点发送。

该实施例的好处是，通过便捷的程序，转换继承的数字资产凭证，提高更新数字资产凭证的效率。

另外，经过上述过程，完成整个继承过程，可以将所述用户的个人安全内核节点设置为终止状态。将所述用户的个人安全内核节点设置为终止状态可以是由智能合约分配节点自动进行的。另外，也可以不在完成上述过程后立即将所述用户的个人安全内核节点设置为终止状态。用户的个人安全内核节点除了在继承中使用，还可能在一些其它的程序中用到。因此，可能除了继承之外，还要等到其它相关程序完成，让所述用户的个人安全内核节点变为终止状态。

用户的个人安全内核节点具有未启用、启用、暂停、终止几种状态。当用户未出生之前，用户的个人安全内核节点相应地处于未启用状态。在用户出生后，经过家长的申请，使该个人安全内核节点处于启用状态。在过程中，如遇到挂失等事件，有可能需要将个人安全内核节点设置到暂停状态，暂停状态下不得对该个人安全内核节点进行操作，直到恢复位置。当用户生命周期结束后，经过上述流程，并完成了其它可能会用到用户的个人安全内核节点的流程后，可以将个人安全内核节点设置为终止状态。终止状态下，该个人安全内核节点被废止，永久不得对该个人安全内核节点进行访问。

另外，有时遗嘱中仅仅指定继承人是不够的，随着继承适用的法律不同，继承的效果可能有很大差别。例如，在某些国家的法律规定，继承交继承税，而另外一些国家的法律规定，继承不交继承税。在一个实施例中，在图 2B 的界面上，用户不仅指定各数字资产凭证对应的继承人个人安全内核节点标识、和执行遗嘱继承的司法机构节点的标识，还指定遗嘱的继承适用法律。这样，在图 2D 所示的遗嘱中，可能还包含该遗嘱的继承适用法律。

在该实施例中，步骤 230 中，所述触发向所述遗嘱中的各继承人个人安全内核节点的标识的继承人个人安全内核节点，发送所述遗嘱中各数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名，包括：

触发向所述遗嘱中的各继承人个人安全内核节点的标识的继承人个人安全内核节点，发送所述遗嘱中各数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名、和遗嘱的继承适用法律，以便所述继承人个人安全内核节点得到继承的数字资产凭证后，执行所述继承适用法律对应的进程。

也就是说，由于遗嘱中还有继承适用法律，因此，触发向遗嘱中的数字资产凭证对应的继承人个人安全内核节点标识的继承人个人安全内核节点，发送的就不仅仅是遗嘱中各数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名，还有遗嘱的继承适用法律。

每一种继承适用法律对应的继承进程可以事先编写好程序代码，存储在公共服务器上或各用户个人安全内核节点中。这样，在一个实施例中，执行所述继承适用法律对应的进程，包括由继承人个人安全内核节点执行的如下过程：根据接收到的继承适用法律，从公共服务器上或继承人个人安全内核节点中获取该继承适用法律对应的程序代码，并将继承的数字资产凭证输入该程序代码，从而执行所述继承适用法律对应的进程。

该实施例的好处是，使得继承能够按照用户指定的继承适用法律进行，提高继承的精细度。

另外，不是所有用户都会在生命周期结束之前设立遗嘱。当用户在生命周期结束之前没有设立遗嘱时，相当于法定继承的情形。除了遗嘱继承的情形，在一个实施例中，还将法定继承的数据处理自动化，实现了自动化缺省遗嘱继承。

如图 5 所示，在一个实施例中，在步骤 210 之后，所述方法还包括：

步骤 225、如果司法机构节点 145 获取不到用户的遗嘱，根据所述用户的个人安全内核节点的身份，确定所述身份对应的法律；

步骤 235、司法机构节点 145 获取所述用户的亲属关系；

步骤 245、司法机构节点 145 获取用户的各数字资产凭证；

步骤 255、针对获取的用户的每一个数字资产凭证，司法机构节点 145 按照确定的法律和所述亲属关系，确定各数字资产凭证对应的继承人个人安全内核节点标识；

步骤 265、司法机构节点 145 获取确定的继承人个人安全内核节点标识的继承人个人安全内核节点的公钥；

步骤 275、司法机构节点 145 将用户的每一个数字资产凭证，用对应的继承人个人安全内核节点的公钥进行签名，并发送到对应的继承人个人安全内核节点，以便所述继承人个人安全内核节点对该签名，用所述继承人个人安全内核节点的私钥解密，得到数字资产凭证的摘要，根据得到的数字资产凭证的摘要，得到继承的数字资产凭证。

下面对这些步骤进行详细描述。

在步骤 225 中，如果司法机构节点 145 获取不到用户的遗嘱，根据所述用户的个人安全内核节点的身份，确定所述身份对应的法律。

如果从区块链或者从用户个人安全内核节点服务器都获取不到用户的遗嘱，很可能用户没来及设立遗嘱就生命周期结束了，此时需要启动法定继承，根据所述用户的个人安全内核节点的身份，确定所述身份对应的法律。

由于用户生命周期结束后，其个人安全内核节点客户端可能找不到，因此，在一个实施例中，要事先将用户的个人安全内核节点的身份存储在个人安全内核节点服务器。根据所述用户的个人安全内核节点的身份，确定所述身份对应的法律，包括：

向启动请求中的用户的个人安全内核节点标识对应的个人安全内核节点服务器发送身份请求；

从所述个人安全内核节点服务器接收用户的个人安全内核节点的身份；

查找身份与法律对应关系表，确定所述身份对应的法律。

由于启动请求中具有用户的个人安全内核节点标识，它对应着唯一一组个人安全内核节点客户端及服务器，因此，可以向启动请求中的用户的个人安全内核节点标识对应的个人安全内核节点服务器发送身份请求。

用户的个人安全内核节点的身份是指用户的国籍、注册地区等。例如，用户是中国人，

可能适用中国法律进行继承。用户是美国人，可能适用美国法律进行继承。

在预定服务器或每个个人安全内核节点中存储用户的个人安全内核节点的身份与继承适用法律的对应关系表，即身份与法律对应关系表。从该对应关系表，可以根据所述用户的个人安全内核节点的身份，确定所述身份对应的法律。

在步骤235中，司法机构节点145获取所述用户的亲属关系。

在一个实施例中，用户的亲属关系列表存储在用户个人安全内核节点服务器中。因此，从该用户个人安全内核节点服务器中的用户的亲属关系列表，可以获取所述用户的亲属关系。

在步骤245中，司法机构节点145获取用户的各数字资产凭证。

在一个实施例中，用户的各数字资产凭证不仅存储在用户个人安全内核节点客户端中，还存储在用户个人安全内核节点服务器中。虽然用户个人安全内核节点客户端可能随着用户生命周期结束后无法找到，但可以按照启动请求中的用户个人安全内核节点，找到对应的用户个人安全内核节点服务器，从中获取用户的各数字资产凭证。

在步骤255中，针对获取的用户的每一个数字资产凭证，司法机构节点145按照确定的法律和所述亲属关系，确定各数字资产凭证对应的继承人个人安全内核节点标识。

在一个实施例中，在专门的服务器中或在每个个人安全内核节点中设置与各适用的法律对应的程序代码。将用户的各数字资产凭证和所述亲属关系输入该与确定的法律对应的程序代码，就得到按照该法律，各数字资产凭证对应的继承人个人安全内核节点标识。

在步骤265中，司法机构节点145获取确定的继承人个人安全内核节点标识的继承人个人安全内核节点的公钥。

在一个实施例中，获取继承人个人安全内核节点标识的继承人个人安全内核节点的公钥可以通过向区块链中专门的认证中心服务器（CA）请求实现。由于认证中心服务器（CA）是发放区块链节点公私钥的节点，可以从其请求任何区块链节点的公钥。

在另一个实施例中，获取确定的继承人个人安全内核节点标识的继承人个人安全内核节点的公钥，包括：从区块链上获取与确定的继承人个人安全内核节点标识对应的继承人个人安全内核节点的公钥，其中，继承人个人安全内核节点的公钥由继承人个人安全内核节点生成，并与继承人个人安全内核节点的公钥标识对应记录在区块链上。

该实施例中，不是由认证中心服务器生成并存储公钥，而是由各个个人安全内核节点生成并发布在区块链上。由于与个人安全内核节点标识对应记录在区块链上，在需要时可以凭个人安全内核节点标识在区块链上查找。

在另一实施例中，获取确定的继承人个人安全内核节点标识的继承人个人安全内核节点的公钥，包括：

通过社交操作系统平台，向继承人好友个人安全内核节点发送公钥获取请求，所述公钥获取请求包括确定的继承人个人安全内核节点标识；

从继承人好友个人安全内核节点，接收该继承人个人安全内核节点标识的继承人个人安全内核节点的公钥。

在社交操作系统平台上（例如微信），当两个用户互相加好友时，其中一个用户的公钥会发到另一个人的个人安全内核节点保存。而社交操作系统平台保存着所有互相加好友的人之间的好友关系。这样，通过社交操作系统平台，可以获取与该继承人个人安全内核节点标识具有好友关系的所有继承人个人安全内核节点标识列表，向该列表中任何一个个人安全内核节点标识的个人安全内核节点发送公钥获取请求，所述公钥获取请求包括确定的继承人个人安全内核节点标识。该个人安全内核节点返回该继承人个人安全内核节点标识的继承人个人安全内核节点的公钥。

在步骤275中，司法机构节点145将用户的每一个数字资产凭证，用对应的继承人个人安全内核节点的公钥进行签名，并发送到对应的继承人个人安全内核节点，以便所述继承人个人安全内核节点对该签名，用所述继承人个人安全内核节点的私钥解密，得到数字资产凭证的摘要，根据得到的数字资产凭证的摘要，得到继承的数字资产凭证。

该步骤与步骤230的区别仅在于，在步骤230中是按照遗嘱中数字资产凭证对应的继

承人安全内核节点发送用对应的继承人个人安全内核节点的公钥进行的签名，而步骤 275 中，是按照法律推导出的数字资产凭证对应的继承人安全内核节点发送用对应的继承人个人安全内核节点的公钥进行签名。大体过程相同，故不赘述。

该实施例的好处是，实现了法定继承的自动化，且保证继承中的安全性。

如图 6 所示，在一个实施例中，所述遗嘱由用户的个人安全内核节点通过以下过程生成：

步骤 410、对于用户的个人安全内核节点中的数字资产凭证，接收用户对该数字资产凭证的继承人个人安全内核节点标识的指定；

步骤 420、获取指定的继承人个人安全内核节点标识的继承人个人安全内核节点的公钥；

步骤 430、将每一个数字资产凭证，用相应获取的指定的继承人个人安全内核节点标识的继承人个人安全内核节点的公钥进行签名，得到各数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名；

步骤 440、将用户个人安全内核节点的标识、各继承人个人安全内核节点的标识、各数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名放入遗嘱中；

步骤 450、接收用户对执行该遗嘱的司法机构节点标识的指定；

步骤 460、获取所述司法机构节点标识的司法机构节点的公钥；

步骤 470、将所述遗嘱中的当前内容用获取的司法机构节点的公钥签名，放入所述遗嘱。

下面，对以上过程进行详细描述。

在步骤 410 中，对于用户的个人安全内核节点中的数字资产凭证，接收用户对该数字资产凭证的继承人个人安全内核节点标识的指定。

图 2B 示出了一个针对个人安全内核节点中的数字资产凭证，用户指定继承人个人安全内核节点标识的界面。实际上，步骤 410 可以通过分类指定或分项指定实现。图 2B 是分项指定的一个例子的界面。

在分项指定的实施例中，步骤 410 包括：

显示用户的个人安全内核节点中的数字资产凭证列表；

针对数字资产凭证列表中的每个数字资产凭证，接收用户对该数字资产凭证的继承人个人安全内核节点标识的指定。

在该实施例中，图 2B 的界面上，向用户显示出包含用户的个人安全内核节点中的所有数字资产凭证的数字资产凭证列表。在列表中的每个数字资产凭证的下面，分别显示了指定对该数字资产凭证的继承人个人安全内核节点标识的下拉框。点击下拉框右部的箭头，下拉菜单弹出，显示了所有候选的继承人个人安全内核节点标识。所有候选的继承人个人安全内核节点标识可以从用户的个人安全内核节点中存储的用户通讯录中直接导出，也可以从用户的个人安全内核节点中存储的亲属关系列表中直接导出。当用户在下拉菜单中选择一个候选个人安全内核节点标识后，就认为指定了对该数字资产凭证的继承人个人安全内核节点标识。

该实施例的好处是便于用户针对每一项数字资产凭证分别指定相应继承人个人安全内核节点标识，提高遗嘱生成的精细度。

在分类指定的实施例中，步骤 410 包括：

显示用户的个人安全内核节点中的数字资产凭证类型列表；

针对数字资产凭证列表中的每个数字资产凭证类型，接收用户对该数字资产凭证类型的继承人个人安全内核节点标识的指定，其中，指定的继承人个人安全内核节点标识用于该数字资产凭证类型的每一个数字资产凭证。

该实施例的界面与图 2B 的不同之处在于，图 2B 的界面显示的是所有数字资产凭证的列表，该实施例的界面显示的是所有数字资产凭证类型（如理财产品单、保险产品单、股票交易单）的列表，这是因为通常用户希望针对同一种类型的数字资产凭证（理财产品单），指定同一个继承人继承。然后，针对数字资产凭证列表中的每个数字资产凭证类型，用户

对该数字资产凭证类型的继承人个人安全内核节点标识进行指定。指定后，这种类型的所有数字资产凭证在继承时都由该指定的继承人个人安全内核节点继承。

该实施例的好处是，针对通常用户希望针对同一种类型的数字资产凭证（理财产品单），指定同一个继承人继承的特点，提高遗嘱生成的效率。

在步骤 420 中，获取指定的继承人个人安全内核节点标识的继承人个人安全内核节点的公钥。

如前所述，获取指定的继承人个人安全内核节点标识的继承人个人安全内核节点的公钥可以向专门的认证中心服务器（CA）请求实现，也可以从区块链上获取，还可以通过社交操作系统平台，向继承人好友个人安全内核节点获取。由于前面已描述具体实现，这里为节约篇幅不再赘述。

在步骤 430 中，将每一个数字资产凭证，用相应获取的指定的继承人个人安全内核节点标识的继承人个人安全内核节点的公钥进行签名，得到各数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名。

如前所述，将数字资产凭证用相应获取的指定的继承人个人安全内核节点标识的继承人个人安全内核节点的公钥进行签名的过程，包括基于预定摘要算法对数字资产凭证生成摘要、和用相应获取的指定的继承人个人安全内核节点标识的继承人个人安全内核节点的公钥对摘要加密的过程。

在步骤 440 中，将用户个人安全内核节点的标识、各继承人个人安全内核节点的标识、各数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名放入遗嘱中。

将用户个人安全内核节点的标识放入遗嘱中是因为，在继承程序中要通过用户个人安全内核节点的标识找回遗嘱。将各继承人个人安全内核节点的标识、各数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名放入遗嘱中，是因为在继承程序中需要向这些标识对应的继承人个人安全内核节点发送数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名。

在步骤 450 中，接收用户对执行该遗嘱的司法机构节点标识的指定。

如图 2B 所示，用户可以在界面中的执行遗嘱的司法机构节点标识下拉框中进行指定。点击下拉框右部的箭头，下拉菜单弹出，显示了所有候选的司法机构节点标识。这些候选的司法机构节点标识是预先导入的。当用户在下拉菜单中选择一个候选司法机构节点标识后，就认为指定了执行该遗嘱的司法机构节点标识。

在步骤 460 中，获取所述司法机构节点标识的司法机构节点的公钥。

与步骤 420 类似，该步骤也可以向专门的认证中心服务器（CA）请求实现，也可以从区块链上获取，还可以通过社交操作系统平台，向继承人好友个人安全内核节点获取，故不赘述。

在步骤 470 中，将所述遗嘱中的当前内容用获取的司法机构节点的公钥签名，放入所述遗嘱。

该签名放入遗嘱的意义如前所述，其在继承程序中可以用来验证执行继承程序的司法机构节点是否是用户真正想要的司法机构节点。如果执行继承程序的司法机构节点不是用户指定的司法机构节点，没有司法机构节点的私钥，无法签名验证成功。

该实施例的好处是，通过快捷的方式，生成遗嘱，提高了遗嘱生成的效率。

如前所述，遗嘱中除了包括用户个人安全内核节点的标识、各继承人个人安全内核节点的标识、各数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名、所述遗嘱用司法机构节点公钥进行的签名之外，还可以包含指定的司法机构节点标识。在该实施例中，在步骤 470 之前，生成遗嘱的方法还包括：将指定的司法机构节点标识放入遗嘱中（未示）。

由于在步骤 450 中，已经接收了用户对执行遗嘱的司法机构节点标识的指定，因此，在本步骤中，可以将该标识放入遗嘱中。

遗嘱在生成后，可以配置在不同的位置。如前所述，在步骤 220 中，获取用户的遗嘱时，可以从区块链上获取，也可以从用户个人安全内核节点服务器获取。实际上，也可以

从用户个人安全内核节点客户端获取，只不过用户个人安全内核节点客户端非常容易随着用户生命周期结束变得找不到，因此，从区块链上或用户个人安全内核节点服务器获取更有保障。在一个实施例中，根据遗嘱配置的安全性要求，可以分成多种安全模式，每种模式安全性等级不同。

在一个实施例中，所述遗嘱生成后通过以下过程配置：

显示安全模式列表，所述安全模式列表包括第一安全模式、第二安全模式、第三安全模式，其中，第一安全模式中，遗嘱存储在用户个人安全内核节点客户端中；第二安全模式中，遗嘱存储在用户个人安全内核节点客户端和服务器中；第三安全模式中，遗嘱存储在用户个人安全内核节点服务器中，并发布在区块链上；

响应于用户在安全模式列表中选择第一安全模式，将所述遗嘱存储在用户个人安全内核节点客户端中；

响应于用户在安全模式列表中选择第二安全模式，将遗嘱存储在用户个人安全内核节点客户端和服务器中；

响应于用户在安全模式列表中选择第三安全模式，将遗嘱存储在用户个人安全内核节点服务器中，并发布在区块链上。

遗嘱的配置是指遗嘱生成后的保存和维护。安全模式是指对应于不同安全性等级的、存储遗嘱的方式。第一安全模式中，遗嘱存储在用户个人安全内核节点客户端中，这样，用户手机丢失后可能找不回数字资产凭证，安全程度最低。第二安全模式中，遗嘱存储在用户个人安全内核节点客户端和服务器中。这样，用户手机丢失仍可找回资产，安全程度其次。第三安全模式中，遗嘱存储在用户个人安全内核节点客户端和服务器中，并发布在区块链上。这样，在其中一处找不到，还可以在另外一处查找，安全程度最高。

另外，当用户在生命周期期间生成了遗嘱后，用户可能会继续生成数字资产凭证，如与依赖方节点形成新的数字资产凭证（如购入新的理财产品，产生新的理财产品单）。对于这些新的数字资产凭证，并没有指定对应的继承人个人安全内核节点标识，因此，在用户生命周期结束后，这些新的数字资产凭证不能根据遗嘱继承。因此，在用户生成遗嘱后，用户个人安全内核节点中数字资产凭证又增加的情况下，可以有让用户补充指定该数字资产凭证的继承人个人安全内核节点标识，和自动为用户指定该数字资产凭证的继承人个人安全内核节点标识两种实施方式。

在让用户补充指定该数字资产凭证的继承人个人安全内核节点标识的实施例中，如图7所示，所述遗嘱由用户的个人安全内核节点通过以下过程更新：

步骤510、当所述用户的个人安全内核节点中增加数字资产凭证时，向用户显示指定该数字资产凭证的继承人个人安全内核节点标识的界面；

步骤520、在所述界面上接收用户对该数字资产凭证的继承人个人安全内核节点标识的指定；

步骤530、获取指定的继承人个人安全内核节点标识的继承人个人安全内核节点的公钥；

步骤540、对增加的数字资产凭证，用相应获取的指定的继承人个人安全内核节点标识的继承人个人安全内核节点的公钥进行签名，得到增加的数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名；

步骤550、将为增加的数字资产凭证指定的继承人个人安全内核节点标识、增加的数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名，添加到遗嘱中；

步骤560、将遗嘱中当前的用获取的司法机构节点的公钥的签名去掉；

步骤570、将所述遗嘱中的当前内容用获取的司法机构节点的公钥签名，放入所述遗嘱。

下面对步骤510-570进行详细描述。

在步骤510中，当所述用户的个人安全内核节点中增加数字资产凭证时，向用户显示指定该数字资产凭证的继承人个人安全内核节点标识的界面。

在一个实施例中，用户的个人安全内核节点中具有检测模块，当有新的数字资产凭证

写入个人安全内核节点（即用户个人安全内核节点与依赖方节点履行业务后产生凭据，即数字资产凭证，写入个人安全内核节点的个人资产保险箱中）时，检测模块会检测到这一情况，显示一个类似于图 2B 的界面，该界面中列出了增加的数字资产凭证，在下面有指定继承人个人安全内核节点的下拉框。点击右部的箭头，可以显示下拉菜单，下拉菜单有所有候选继承人个人安全内核节点标识的列表，让用户选择。

在步骤 520 中，在所述界面上接收用户对该数字资产凭证的继承人个人安全内核节点标识指定。

当用户在下拉菜单中选择一个继承人个人安全内核节点标识，就认为接收到了用户对该数字资产凭证的继承人个人安全内核节点标识的指定。

在步骤 530 中，获取指定的继承人个人安全内核节点标识的继承人个人安全内核节点的公钥。

与步骤 420 类似，该步骤也可以向专门的认证中心服务器（CA）请求实现，也可以从区块链上获取，还可以通过社交操作系统平台，向继承人好友个人安全内核节点获取，故不赘述。

在步骤 540 中，对增加的数字资产凭证，用相应获取的指定的继承人个人安全内核节点标识的继承人个人安全内核节点的公钥进行签名，得到增加的数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名。

该步骤与步骤 430 类似，包括按预定的摘要算法生成增加的数字资产凭证的摘要，并用相应获取的指定的继承人个人安全内核节点标识的继承人个人安全内核节点的公钥对摘要加密的过程。

在步骤 550 中，将为增加的数字资产凭证指定的继承人个人安全内核节点标识、增加的数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名，添加到遗嘱中。

该步骤与步骤 440 类似，只不过步骤 550 是仅对增加的数字资产凭证，执行将继承人个人安全内核节点标识和相应签名增加到遗嘱中，故不赘述。

在步骤 560 中，将遗嘱中当前的用获取的司法机构节点的公钥的签名去掉。

由于在 470 中生成遗嘱用司法机构节点的公钥的签名时，是针对当时生成遗嘱时遗嘱中的当前内容进行的签名，在由于遗嘱当前内容增加了步骤 550 中添加的内容，导致签名继承有变化，因此，需要重新签名。但是遗嘱中该签名本身不是签名基础的一部分，在形成新的遗嘱用司法机构节点的公钥的签名时，首先要将该签名去掉，在此基础上，将所述遗嘱中的当前内容用获取的司法机构节点的公钥签名。这时的当前内容就包括了步骤 550 中添加的内容。

在步骤 570 中，将所述遗嘱中的当前内容用获取的司法机构节点的公钥签名，放入所述遗嘱。

上述过程在遗嘱生成后用户的数字资产凭证增加的情况下，提供了一种简单易行的更新遗嘱的方式，避免了遗嘱中一些新增加的数字资产凭证将来可能没有继承人的问题。

在自动为新增加的数字资产凭证补充该数字资产凭证的继承人个人安全内核节点标识的情况下，在一个实施例中，如图 8 所示，所述遗嘱由用户的个人安全内核节点通过以下过程更新：

步骤 510’、当所述用户的个人安全内核节点中增加数字资产凭证时，根据遗嘱中为已有的数字资产凭证指定的继承人个人安全内核节点标识，确定增加的数字资产凭证对应的继承人个人安全内核节点标识；

步骤 520’、获取增加的数字资产凭证对应的继承人个人安全内核节点标识的继承人个人安全内核节点的公钥；

步骤 530’、对增加的数字资产凭证，用相应获取的指定的继承人个人安全内核节点标识的继承人个人安全内核节点的公钥进行签名，得到增加的数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名；

步骤 540’、将为增加的数字资产凭证指定的继承人个人安全内核节点标识、增加的数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名，添加到遗嘱中；

步骤550’、将遗嘱中当前的用获取的司法机构节点的公钥的签名去掉；

步骤560’、将所述遗嘱中的当前内容用获取的司法机构节点的公钥签名，放入所述遗嘱。

下面对上述步骤进行详细描述。

在步骤510’中，当所述用户的个人安全内核节点中增加数字资产凭证时，根据遗嘱中为已有的数字资产凭证指定的继承人个人安全内核节点标识，确定增加的数字资产凭证对应的继承人个人安全内核节点标识。

判断所述用户的个人安全内核节点中增加数字资产凭证的方法与步骤510相同。

在一个实施例中，所述根据遗嘱中为已有的数字资产凭证指定的继承人个人安全内核节点标识，确定增加的数字资产凭证对应的继承人个人安全内核节点标识，包括：

获取增加的数字资产凭证的类型；

查找遗嘱中已为相同类型的数字资产凭证指定的继承人个人安全内核节点标识；

如果遗嘱中已为相同类型的数字资产凭证指定的继承人个人安全内核节点标识一致，将遗嘱中已为相同类型的数字资产凭证指定的继承人个人安全内核节点标识确定为增加的数字资产凭证对应的继承人个人安全内核节点标识。

由于数字资产凭证中含有数字资产凭证的类型字段，因此，从该数字资产凭证的类型字段可以获取增加的数字资产凭证的类型。

例如，增加的数字资产凭证的类型为理财产品，查找遗嘱中已为理财产品类型的数字资产凭证指定继承人个人安全内核节点标识。如果遗嘱中之前有5个理财产品类型的数字资产凭证，为这些数字资产凭证指定的继承人个人安全内核节点标识就有5个，但这5个可能是相同的继承人个人安全内核节点标识。即，遗嘱中已为相同类型的数字资产凭证指定的继承人个人安全内核节点标识一致，这时，用户很可能希望对于新增加的数字资产凭证也指定同样的继承人个人安全内核节点继承，因此，将遗嘱中已为相同类型的数字资产凭证指定的继承人个人安全内核节点标识确定为增加的数字资产凭证对应的继承人个人安全内核节点标识。

在一个实施例中，所述根据遗嘱中为已有的数字资产凭证指定的继承人个人安全内核节点标识，确定增加的数字资产凭证对应的继承人个人安全内核节点标识，还包括：

如果遗嘱中已为相同类型的数字资产凭证指定的继承人个人安全内核节点标识不一致，将遗嘱中已为相同类型的数字资产凭证指定的多个继承人个人安全内核节点标识中最多的继承人个人安全内核节点标识，确定为增加的数字资产凭证对应的继承人个人安全内核节点标识。

例如，如果遗嘱中之前有5个理财产品类型的数字资产凭证，为这些数字资产凭证指定的继承人个人安全内核节点标识就有5个，其中3个是继承人个人安全内核节点A的标识，2个是继承人个人安全内核节点B的标识，这时两者多的一个，可能是用户更希望指定的，因此，自动将将遗嘱中已为相同类型的数字资产凭证指定的5个继承人个人安全内核节点标识中最多的继承人个人安全内核节点标识，即继承人个人安全内核节点A的标识，确定为增加的数字资产凭证对应的继承人个人安全内核节点标识。

该实施例基于之前为相同类型的数字资产凭证指定的继承人个人安全内核节点标识，来确定为新增加的数字资产凭证指定的继承人个人安全内核节点标识，由于用户倾向于对于同类数字资产凭证，指定同一继承人个人安全内核节点，该实施例提高了自动指定继承人个人安全内核节点标识的准确性。

另外，如果遗嘱中没有找到相同类型的数字资产凭证，则可以按照类似步骤510-520的方式，让用户手动选择希望增加的数字资产凭证对应的继承人个人安全内核节点标识。

在一个实施例中，所述根据遗嘱中为已有的数字资产凭证指定的继承人个人安全内核节点标识，确定增加的数字资产凭证对应的继承人个人安全内核节点标识，包括：

获取增加的数字资产凭证的业务依赖方节点标识；

查找遗嘱中已为相同业务依赖方节点标识的数字资产凭证指定的继承人个人安全内核节点标识；

如果遗嘱中已为相同业务依赖方节点标识的数字资产凭证指定的继承人个人安全内核节点标识一致，将遗嘱中已为相同业务依赖方节点标识的数字资产凭证指定的继承人个人安全内核节点标识确定为增加的数字资产凭证对应的继承人个人安全内核节点标识。

由于数字资产凭证中也含有业务依赖方节点标识字段，因此，从该依赖方节点标识字段可以获取增加的数字资产凭证的业务依赖方节点标识。

例如，增加的数字资产凭证是一个从理财公司 A 购买的理财产品，因此，业务依赖方节点标识是理财公司 A 的终端标识。查找遗嘱中为从理财公司 A 终端形成的数字资产凭证（例如理财产品等）指定的继承人个人安全内核节点标识有 5 个，但这 5 个可能是相同的继承人个人安全内核节点标识，这时就将该相同的继承人个人安全内核节点标识作为增加的数字资产凭证对应的继承人个人安全内核节点标识。

在一个实施例中，所述根据遗嘱中为已有的数字资产凭证指定的继承人个人安全内核节点标识，确定增加的数字资产凭证对应的继承人个人安全内核节点标识，还包括：

如果遗嘱中已为相同业务依赖方节点标识的数字资产凭证指定的继承人个人安全内核节点标识不一致，将遗嘱中已为相同业务依赖方节点标识的数字资产凭证指定的多个继承人个人安全内核节点标识中最多的继承人个人安全内核节点标识，确定为增加的数字资产凭证对应的继承人个人安全内核节点标识。

例如，如果遗嘱中之前有 5 个理财产品是从理财公司 A 购买的，为这些数字资产凭证指定的继承人个人安全内核节点标识就有 5 个，其中 3 个是继承人个人安全内核节点 A 的标识，2 个是继承人个人安全内核节点 B 的标识，这时两者多的一个，可能是用户更希望指定的，因此，自动将将遗嘱中已为相同业务依赖方节点标识的数字资产凭证指定的 5 个继承人个人安全内核节点标识中最多的继承人个人安全内核节点标识，即继承人个人安全内核节点 A 的标识，确定为增加的数字资产凭证对应的继承人个人安全内核节点标识。

该实施例基于之前为相同业务依赖方节点标识的数字资产凭证指定的继承人个人安全内核节点标识，来确定为新增加的数字资产凭证指定的继承人个人安全内核节点标识，由于用户倾向于对于同一业务依赖方节点的数字资产凭证，指定同一继承人个人安全内核节点，该实施例提高了自动指定继承人个人安全内核节点标识的准确性。

在步骤 520’中，获取增加的数字资产凭证对应的继承人个人安全内核节点标识的继承人个人安全内核节点的公钥。

与步骤 530 类似，该步骤也可以向专门的认证中心服务器（CA）请求实现，也可以从区块链上获取，还可以通过社交操作系统平台，向继承人好友个人安全内核节点获取，故不赘述。

在步骤 530’中，对增加的数字资产凭证，用相应获取的指定的继承人个人安全内核节点标识的继承人个人安全内核节点的公钥进行签名，得到增加的数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名。

该步骤与步骤 540 类似，故不赘述。

在步骤 540’中，将为增加的数字资产凭证指定的继承人个人安全内核节点标识、增加的数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名，添加到遗嘱中。

该步骤与步骤 550 类似，故不赘述。

在步骤 550’中，将遗嘱中当前的用获取的司法机构节点的公钥的签名去掉。

该步骤与步骤 560 类似，故不赘述。

在步骤 560’中，将所述遗嘱中的当前内容用获取的司法机构节点的公钥签名，放入所述遗嘱。

该步骤与步骤 570 类似，故不赘述。

该实施例实现了自动根据用户个人安全内核节点中已有的数字资产凭证，为新增加的数字资产凭证分配继承人个人安全内核节点标识，提高了遗嘱更新的自动化程度。

另外，如果遗嘱中没有找到相同业务依赖方节点标识的数字资产凭证，则可以按照类似步骤 510-520 的方式，让用户手动选择希望增加的数字资产凭证对应的继承人个人安全内核节点标识。

如图 9 所示，根据一个实施例，还提供了一种司法机构节点，包括：

生命周期结束确定单元 610，用于确定用户的生命周期结束；

遗嘱获取单元 620，用于获取用户的遗嘱，所述遗嘱包括用户个人安全内核节点的标识、各继承人个人安全内核节点的标识、各数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名、所述遗嘱用司法机构节点公钥进行的签名；

第一数字资产凭证签名发送单元 630，用于如果对所述遗嘱用司法机构节点公钥进行的签名，用司法机构节点私钥进行签名验证成功，触发向所述遗嘱中的各继承人个人安全内核节点的标识的继承人个人安全内核节点，发送所述遗嘱中各数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名，以便所述继承人个人安全内核节点对该签名，用所述继承人个人安全内核节点的私钥解密，得到数字资产凭证的摘要，根据得到的数字资产凭证的摘要，得到继承的数字资产凭证。

在一个实施例中，所述生命周期结束确定单元 610 进一步用于：

响应于来自调查节点的生命周期结束通知，确定用户的生命周期结束。

在一个实施例中，所述生命周期结束确定单元 610 进一步用于：

接收到启动节点的启动请求；

通过社交操作系统平台，向多个证明方节点发送继承程序启动确认请求；

如果所述多个证明方节点的应答满足预定条件，则确定用户的生命周期结束。

在一个实施例中，所述如果所述多个证明方节点的应答满足预定条件，则确定用户的生命周期结束，包括：

如果所述多个证明方节点的应答满足预定条件，且接收到来自调查节点的生命周期结束通知，则确定用户的生命周期结束。

在一个实施例中，所述遗嘱还包括指定的执行该遗嘱的司法机构节点标识。所述对所述遗嘱用司法机构节点公钥进行的签名，用司法机构节点私钥进行签名验证成功，包括：

获取遗嘱中指定的执行该遗嘱的司法机构节点标识；

如果遗嘱中指定的执行该遗嘱的司法机构节点标识是当前执行所述方法的司法机构节点的标识，对所述遗嘱用司法机构节点公钥进行的签名，用司法机构节点私钥进行签名验证成功。

在一个实施例中，所述如果遗嘱中指定的执行该遗嘱的司法机构节点标识是当前执行所述方法的司法机构节点的标识，对所述遗嘱用司法机构节点公钥进行的签名，用司法机构节点私钥进行签名验证成功，包括：

如果遗嘱中指定的执行该遗嘱的司法机构节点标识是当前执行所述方法的司法机构节点的标识，对所述遗嘱用司法机构节点公钥进行的签名，用司法机构节点私钥解密，得到解密后产生的遗嘱摘要；

生成所述遗嘱的摘要；

如果解密后产生的遗嘱摘要与生成的遗嘱的摘要一致，则确定对所述遗嘱用司法机构节点公钥进行的签名，用司法机构节点私钥进行签名验证成功。

在一个实施例中，所述继承的数字资产凭证中包含数字资产凭证依赖的业务依赖方节点标识，以便所述继承人个人安全内核节点与该业务依赖方节点标识的业务依赖方节点，根据继承的数字资产凭证，生成继承人节点与该业务依赖方节点之间的更新后数字资产凭证。

在一个实施例中，所述遗嘱还包括所述遗嘱的继承适用法律，所述触发向所述遗嘱中的各继承人个人安全内核节点的标识的继承人个人安全内核节点，发送所述遗嘱中各数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名，包括：

触发向所述遗嘱中的各继承人个人安全内核节点的标识的继承人个人安全内核节点，发送所述遗嘱中各数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名、和遗嘱的继承适用法律，以便所述继承人个人安全内核节点得到继承的数字资产凭证后，执行所述继承适用法律对应的进程。

在一个实施例中，所述司法机构节点还包括：

身份对应法律确定单元，用于如果获取不到用户的遗嘱，根据所述用户的个人安全内核节点的身份，确定所述身份对应的法律；

亲属关系获取单元，用于获取所述用户的亲属关系；

数字资产凭证获取单元，用于获取用户的各数字资产凭证；

继承人个人安全内核节点标识确定单元，用于针对获取的用户的每一个数字资产凭证，按照确定的法律和所述亲属关系，确定各数字资产凭证对应的继承人个人安全内核节点标识；

继承人个人安全内核节点公钥获取单元，用于获取确定的继承人个人安全内核节点标识的继承人个人安全内核节点的公钥；

第二数字资产凭证签名发送单元，用于将用户的每一个数字资产凭证，用对应的继承人个人安全内核节点的公钥进行签名，并发送到对应的继承人个人安全内核节点，以便所述继承人个人安全内核节点对该签名，用所述继承人个人安全内核节点的私钥解密，得到数字资产凭证的摘要，根据得到的数字资产凭证的摘要，得到继承的数字资产凭证。

在一个实施例中，所述遗嘱由用户的个人安全内核节点通过以下过程生成：

对于用户的个人安全内核节点中的数字资产凭证，接收用户对该数字资产凭证的继承人个人安全内核节点标识的指定；

获取指定的继承人个人安全内核节点标识的继承人个人安全内核节点的公钥；

将每一个数字资产凭证，用相应获取的指定的继承人个人安全内核节点标识的继承人个人安全内核节点的公钥进行签名，得到各数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名；

将用户个人安全内核节点的标识、各继承人个人安全内核节点的标识、各数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名放入遗嘱中；

接收用户对执行该遗嘱的司法机构节点标识的指定；

获取所述司法机构节点标识的司法机构节点的公钥；

将所述遗嘱中的当前内容用获取的司法机构节点的公钥签名，放入所述遗嘱。

在一个实施例中，在将所述遗嘱用获取的司法机构节点的公钥签名，放入所述遗嘱之前，所述的遗嘱的生成过程还包括：

将指定的司法机构节点标识放入遗嘱中。

在一个实施例中，所述遗嘱生成后通过以下过程配置：

显示安全模式列表，所述安全模式列表包括第一安全模式、第二安全模式、第三安全模式，其中，第一安全模式中，遗嘱存储在用户个人安全内核节点客户端中；第二安全模式中，遗嘱存储在用户个人安全内核节点客户端和服务器中；第三安全模式中，遗嘱存储在用户个人安全内核节点服务器中，并发布在区块链上；

响应于用户在安全模式列表中选择第一安全模式，将所述遗嘱存储在用户个人安全内核节点客户端中；

响应于用户在安全模式列表中选择第二安全模式，将遗嘱存储在用户个人安全内核节点客户端和服务器中；

响应于用户在安全模式列表中选择第三安全模式，将遗嘱存储在用户个人安全内核节点服务器中，并发布在区块链上。

在一个实施例中，所述遗嘱由用户的个人安全内核节点通过以下过程更新：

当所述用户的个人安全内核节点中增加数字资产凭证时，向用户显示指定该数字资产凭证的继承人个人安全内核节点标识的界面；

在所述界面上接收用户对该数字资产凭证的继承人个人安全内核节点标识的指定；

获取指定的继承人个人安全内核节点标识的继承人个人安全内核节点的公钥；

对增加的数字资产凭证，用相应获取的指定的继承人个人安全内核节点标识的继承人个人安全内核节点的公钥进行签名，得到增加的数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名；

将为增加的数字资产凭证指定的继承人个人安全内核节点标识、增加的数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名，添加到遗嘱中；

将遗嘱中当前的用获取的司法机构节点的公钥的签名去掉；

将所述遗嘱中的当前内容用获取的司法机构节点的公钥签名，放入所述遗嘱。

在一个实施例中，所述遗嘱由用户的个人安全内核节点通过以下过程更新：

当所述用户的个人安全内核节点中增加数字资产凭证时，根据遗嘱中为已有的数字资产凭证指定的继承人个人安全内核节点标识，确定增加的数字资产凭证对应的继承人个人安全内核节点标识；

获取增加的数字资产凭证对应的继承人个人安全内核节点标识的继承人个人安全内核节点的公钥；

对增加的数字资产凭证，用相应获取的指定的继承人个人安全内核节点标识的继承人个人安全内核节点的公钥进行签名，得到增加的数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名；

将为增加的数字资产凭证指定的继承人个人安全内核节点标识、增加的数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名，添加到遗嘱中；

将遗嘱中当前的用获取的司法机构节点的公钥的签名去掉；

将所述遗嘱中的当前内容用获取的司法机构节点的公钥签名，放入所述遗嘱。

根据本申请实施例的数字资产凭证继承转移中的信息处理方法可以由图 10 的司法机构节点 145 实现。

如图 10 所示，司法机构节点 145 以通用计算设备的形式表现。司法机构节点 145 的组件可以包括但不限于：上述至少一个处理单元 810、上述至少一个存储单元 820、连接不同系统组件（包括存储单元 820 和处理单元 810）的总线 830。

其中，所述存储单元存储有程序代码，所述程序代码可以被所述处理单元 810 执行，使得所述处理单元 810 执行本说明书上述示例性方法的描述部分中描述的根据本发明各种示例性实施方式的步骤。例如，所述处理单元 810 可以执行如图 3 中所示的各个步骤。

存储单元 820 可以包括易失性存储单元形式的可读介质，例如随机存取存储单元（RAM）8201 和/或高速缓存存储单元 8202，还可以进一步包括只读存储单元（ROM）8203。

存储单元 820 还可以包括具有一组（至少一个）程序模块 8205 的程序/实用工具 8204，这样的程序模块 8205 包括但不限于：社交操作系统、一个或者多个应用程序、其它程序模块以及程序数据，这些示例中的每一个或某种组合中可能包括网络环境的实现。

总线 830 可以为表示几类总线结构中的一种或多种，包括存储单元总线或者存储单元控制器、外围总线、图形加速端口、处理单元或者使用多种总线结构中的任意总线结构的局域总线。

司法机构节点 145 也可以与一个或多个外部设备 700（例如键盘、指向设备、蓝牙设备等）通信，还可与一个或者多个使得用户能与该司法机构节点 145 交互的设备通信，和/或与使得该司法机构节点 145 能与一个或多个其它计算设备进行通信的任何设备（例如路由器、调制解调器等等）通信。这种通信可以通过输入/输出（I/O）接口 850 进行。并且，司法机构节点 145 还可以通过网络适配器 860 与一个或者多个网络（例如局域网（LAN），广域网（WAN）和/或公共网络，例如因特网）通信。如图所示，网络适配器 860 通过总线 830 与司法机构节点 145 的其它模块通信。应当明白，尽管图中未示出，可以结合司法机构节点 145 使用其它硬件和/或软件模块，包括但不限于：微代码、设备驱动器、冗余处理单元、外部磁盘驱动阵列、RAID 系统、磁带驱动器以及数据备份存储系统等。

通过以上的实施方式的描述，本领域的技术人员易于理解，这里描述的示例实施方式可以通过软件实现，也可以通过软件结合必要的硬件的方式来实现。因此，根据本申请实施方式的技术方案可以以软件产品的形式体现出来，该软件产品可以存储在一个非易失性存储介质（可以是 CD-ROM，U 盘，移动硬盘等）中或网络上，包括若干指令以使得一台计算设备（可以是个人计算机、服务器、终端装置、或者网络设备等）执行根据本申请实施方式的方法。

在本申请的示例性实施例中，还提供了一种计算机程序介质，其上存储有计算机可读指令，当所述计算机可读指令被计算机的处理器执行时，使计算机执行上述方法实施例部分描述的方法。

在本申请的示例性实施例中，还提供了一种包括指令的计算机程序产品，当其在计算机上运行时，使得所述计算机执行上述方法实施例部分描述的方法。

其中，所述计算机程序产品可以采用便携式紧凑盘只读存储器(CD-ROM)并包括程序代码，并可以在终端设备，例如个人电脑上运行。然而，本发明的程序产品不限于此，在本文件中，可读存储介质可以是任何包含或存储程序的有形介质，该程序可以被指令执行系统、装置或者器件使用或者与其结合使用。

所述程序产品可以采用一个或多个可读介质的任意组合。可读介质可以是可读信号介质或者可读存储介质。可读存储介质例如可以为但不限于电、磁、光、电磁、红外线、或半导体的系统、装置或器件，或者任意以上的组合。可读存储介质的更具体的例子（非穷举的列表）包括：具有一个或多个导线的电连接、便携式盘、硬盘、随机存取存储器（RAM）、只读存储器（ROM）、可擦式可编程只读存储器（EPROM 或闪存）、光纤、便携式紧凑盘只读存储器(CD-ROM)、光存储器件、磁存储器件、或者上述的任意合适的组合。

计算机可读信号介质可以包括在基带中或者作为载波一部分传播的数据信号，其中承载了可读程序代码。这种传播的数据信号可以采用多种形式，包括但不限于电磁信号、光信号或上述的任意合适的组合。可读信号介质还可以是可读存储介质以外的任何可读介质，该可读介质可以发送、传播或者传输用于由指令执行系统、装置或者器件使用或者与其结合使用的程序。

可读介质上包含的程序代码可以用任何适当的介质传输，包括但不限于无线、有线、光缆、RF 等等，或者上述的任意合适的组合。

可以以一种或多种程序设计语言的任意组合来编写用于执行本发明操作的程序代码，所述程序设计语言包括面向对象的程序设计语言—诸如 Java、C++等，还包括常规的过程式程序设计语言—诸如“C”语言或类似的程序设计语言。程序代码可以完全地在用户计算设备上执行、部分地在用户设备上执行、作为一个独立的软件包执行、部分在用户计算设备上部分在远程计算设备上执行、或者完全在远程计算设备或服务器上执行。在涉及远程计算设备的情形中，远程计算设备可以通过任意种类的网络，包括局域网（LAN）或广域网（WAN），连接到用户计算设备，或者，可以连接到外部计算设备（例如利用因特网服务提供商来通过因特网连接）。

应当注意，尽管在上文详细描述中提及了用于动作执行的设备的若干模块或者单元，但是这种划分并非强制性的。实际上，根据本申请的实施方式，上文描述的两个或更多模块或者单元的特征和功能可以在一个模块或者单元中具体化。反之，上文描述的一个模块或者单元的特征和功能可以进一步划分为由多个模块或者单元来具体化。

此外，尽管在附图中以特定顺序描述了本申请中方法的各个步骤，但是，这并非要求或者暗示必须按照该特定顺序来执行这些步骤，或是必须执行全部所示的步骤才能实现期望的结果。附加的或备选的，可以省略某些步骤，将多个步骤合并为一个步骤执行，以及/或者将一个步骤分解为多个步骤执行等。

通过以上的实施方式的描述，本领域的技术人员易于理解，这里描述的示例实施方式可以通过软件实现，也可以通过软件结合必要的硬件的方式来实现。因此，根据本申请实施方式的技术方案可以以软件产品的形式体现出来，该软件产品可以存储在一个非易失性存储介质（可以是 CD-ROM，U 盘，移动硬盘等）中或网络上，包括若干指令以使得一台计算设备（可以是个人计算机、服务器、移动终端、或者网络设备等）执行根据本申请实施方式的方法。

本领域技术人员在考虑说明书及实践这里公开的发明后，将容易想到本申请的其它实施方案。本申请旨在涵盖本申请的任何变型、用途或者适应性变化，这些变型、用途或者适应性变化遵循本申请的一般性原理并包括本申请未公开的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的，本申请的真正范围和精神由所附的权利

要求指出。

权 利 要 求

1、一种数字资产凭证继承转移中的信息处理方法，所述方法由司法机构节点执行，所述方法包括：

确定用户的生命周期结束；

获取用户的遗嘱，所述遗嘱包括用户个人安全内核节点的标识、各继承人个人安全内核节点的标识、各数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名、所述遗嘱用司法机构节点公钥进行的签名；

如果对所述遗嘱用司法机构节点公钥进行的签名，用司法机构节点私钥进行签名验证成功，触发向所述遗嘱中的各继承人个人安全内核节点的标识的继承人个人安全内核节点，发送所述遗嘱中各数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名，以便所述继承人个人安全内核节点对该签名，用所述继承人个人安全内核节点的私钥解密，得到数字资产凭证的摘要，根据得到的数字资产凭证的摘要，得到继承的数字资产凭证。

2、根据权利要求 1 所述的方法，所述确定用户的生命周期结束，包括：

响应于来自调查节点的生命周期结束通知，确定用户的生命周期结束。

3、根据权利要求 1 所述的方法，所述确定用户的生命周期结束，包括：

接收到启动节点的启动请求；

通过社交操作系统平台，向多个证明方节点发送继承程序启动确认请求；

如果所述多个证明方节点的应答满足预定条件，则确定用户的生命周期结束。

4、根据权利要求 3 所述的方法，所述如果所述多个证明方节点的应答满足预定条件，则确定用户的生命周期结束，包括：

如果所述多个证明方节点的应答满足预定条件，且接收到来自调查节点的生命周期结束通知，则确定用户的生命周期结束。

5、根据权利要求 1 所述的方法，所述遗嘱还包括指定的执行该遗嘱的司法机构节点标识，所述对所述遗嘱用司法机构节点公钥进行的签名，用司法机构节点私钥进行签名验证成功，包括：

获取遗嘱中指定的执行该遗嘱的司法机构节点标识；

如果遗嘱中指定的执行该遗嘱的司法机构节点标识是当前执行所述方法的司法机构节点的标识，对所述遗嘱用司法机构节点公钥进行的签名，用司法机构节点私钥进行签名验证成功。

6、根据权利要求 5 所述的方法，所述如果遗嘱中指定的执行该遗嘱的司法机构节点标识是当前执行所述方法的司法机构节点的标识，对所述遗嘱用司法机构节点公钥进行的签名，用司法机构节点私钥进行签名验证成功，包括：

如果遗嘱中指定的执行该遗嘱的司法机构节点标识是当前执行所述方法的司法机构节点的标识，对所述遗嘱用司法机构节点公钥进行的签名，用司法机构节点私钥解密，得到解密后产生的遗嘱摘要；

生成所述遗嘱的摘要；

如果解密后产生的遗嘱摘要与生成的遗嘱的摘要一致，则确定对所述遗嘱用司法机构节点公钥进行的签名，用司法机构节点私钥进行签名验证成功。

7、根据权利要求 1 所述的方法，所述继承的数字资产凭证中包含数字资产凭证依赖的业务依赖方节点标识，以便所述继承人个人安全内核节点与该业务依赖方节点标识的业务依赖方节点，根据继承的数字资产凭证，生成继承人节点与该业务依赖方节点之间的更新后数字资产凭证。

8、根据权利要求 1 所述的方法，所述遗嘱还包括所述遗嘱的继承适用法律，所述触发向所述遗嘱中的各继承人个人安全内核节点的标识的继承人个人安全内核节点，发送所述遗嘱中各数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名，包括：

触发向所述遗嘱中的各继承人个人安全内核节点的标识的继承人个人安全内核节点，发送所述遗嘱中各数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名、和遗嘱的继承适用法律，以便所述继承人个人安全内核节点得到继承的数字资产凭证后，执行

所述继承适用法律对应的进程。

9、根据权利要求 1 所述的方法，在确定用户的生命周期结束之后，所述方法还包括：

如果获取不到用户的遗嘱，根据所述用户的个人安全内核节点的身份，确定所述身份对应的法律；

获取所述用户的亲属关系；

获取用户的各数字资产凭证；

针对获取的用户的每一个数字资产凭证，按照确定的法律和所述亲属关系，确定各数字资产凭证对应的继承人个人安全内核节点标识；

获取确定的继承人个人安全内核节点标识的继承人个人安全内核节点的公钥；

将用户的每一个数字资产凭证，用对应的继承人个人安全内核节点的公钥进行签名，并发送到对应的继承人个人安全内核节点，以便所述继承人个人安全内核节点对该签名，用所述继承人个人安全内核节点的私钥解密，得到数字资产凭证的摘要，根据得到的数字资产凭证的摘要，得到继承的数字资产凭证。

10、根据权利要求 1 所述的方法，所述遗嘱由用户的个人安全内核节点通过以下过程生成：

对于用户的个人安全内核节点中的数字资产凭证，接收用户对该数字资产凭证的继承人个人安全内核节点标识的指定；

获取指定的继承人个人安全内核节点标识的继承人个人安全内核节点的公钥；

将每一个数字资产凭证，用相应获取的指定的继承人个人安全内核节点标识的继承人个人安全内核节点的公钥进行签名，得到各数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名；

将用户个人安全内核节点的标识、各继承人个人安全内核节点的标识、各数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名放入遗嘱中；

接收用户对执行该遗嘱的司法机构节点标识的指定；

获取所述司法机构节点标识的司法机构节点的公钥；

将所述遗嘱中的当前内容用获取的司法机构节点的公钥签名，放入所述遗嘱。

11、根据权利要求 10 所述的方法，所述遗嘱生成后通过以下过程配置：

显示安全模式列表，所述安全模式列表包括第一安全模式、第二安全模式、第三安全模式，其中，第一安全模式中，遗嘱存储在用户个人安全内核节点客户端中；第二安全模式中，遗嘱存储在用户个人安全内核节点客户端和服务器中；第三安全模式中，遗嘱存储在用户个人安全内核节点服务器中，并发布在区块链上；

响应于用户在安全模式列表中选择第一安全模式，将所述遗嘱存储在用户个人安全内核节点客户端中；

响应于用户在安全模式列表中选择第二安全模式，将遗嘱存储在用户个人安全内核节点客户端和服务器中；

响应于用户在安全模式列表中选择第三安全模式，将遗嘱存储在用户个人安全内核节点服务器中，并发布在区块链上。

12、根据权利要求 10 所述的方法，所述遗嘱由用户的个人安全内核节点通过以下过程更新：

当所述用户的个人安全内核节点中增加数字资产凭证时，根据遗嘱中为已有的数字资产凭证指定的继承人个人安全内核节点标识，确定增加的数字资产凭证对应的继承人个人安全内核节点标识；

获取增加的数字资产凭证对应的继承人个人安全内核节点标识的继承人个人安全内核节点的公钥；

对增加的数字资产凭证，用相应获取的指定的继承人个人安全内核节点标识的继承人个人安全内核节点的公钥进行签名，得到增加的数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名；

将为增加的数字资产凭证指定的继承人个人安全内核节点标识、增加的数字资产凭证

用对应继承人个人安全内核节点的公钥进行的签名，添加到遗嘱中；

将遗嘱中当前的用获取的司法机构节点的公钥的签名去掉；

将所述遗嘱中的当前内容用获取的司法机构节点的公钥签名，放入所述遗嘱。

13、一种司法机构节点，包括：

生命周期结束确定单元，用于确定用户的生命周期结束；

遗嘱获取单元，用于获取用户的遗嘱，所述遗嘱包括用户个人安全内核节点的标识、各继承人个人安全内核节点的标识、各数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名、所述遗嘱用司法机构节点公钥进行的签名；

第一数字资产凭证签名发送单元，用于如果对所述遗嘱用司法机构节点公钥进行的签名，用司法机构节点私钥进行签名验证成功，触发向所述遗嘱中的各继承人个人安全内核节点的标识的继承人个人安全内核节点，发送所述遗嘱中各数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名，以便所述继承人个人安全内核节点对该签名，用所述继承人个人安全内核节点的私钥解密，得到数字资产凭证的摘要，根据得到的数字资产凭证的摘要，得到继承的数字资产凭证

14、一种数字资产凭证继承转移中的信息处理方法，所述方法由司法机构节点执行，所述方法包括：

当用户的个人安全内核节点中增加数字资产凭证时，获取增加的数字资产凭证对应的继承人个人安全内核节点标识，以及所述继承人个人安全内核节点标识的继承人个人安全内核节点的公钥；

对增加的数字资产凭证，用所述继承人个人安全内核节点的公钥进行签名，得到增加的数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名；

将所述继承人个人安全内核节点标识、增加的数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名，添加到所述用户的遗嘱中，所述遗嘱中包含有用司法机构节点公钥进行的签名；

将所述遗嘱中包含的用司法机构节点公钥进行的签名去掉；

将所述遗嘱中的当前内容用所述司法机构节点公钥进行签名，并将得到的签名放入所述遗嘱。

15、根据权利要求 14 所述的方法，所述获取增加的数字资产凭证对应的继承人个人安全内核节点标识，以及所述继承人个人安全内核节点标识的继承人个人安全内核节点的公钥，包括：

向用户显示指定增加的数字资产凭证的继承人个人安全内核节点标识的界面；

在所述界面上接收用户对所述增加的数字资产凭证的继承人个人安全内核节点标识的指定；

获取用户指定的继承人个人安全内核节点标识的继承人个人安全内核节点的公钥。

16、根据权利要求 15 所述的方法，所述获取用户指定的继承人个人安全内核节点标识的继承人个人安全内核节点的公钥，包括：

向区块链中的认证中心服务器请求获取用户指定的继承人个人安全内核节点标识的继承人个人安全内核节点的公钥；或者

从区块链上获取与用户指定的继承人个人安全内核节点标识对应的继承人个人安全内核节点的公钥，其中，继承人个人安全内核节点的公钥由继承人个人安全内核节点生成，并与继承人个人安全内核节点的公钥标识对应记录在区块链上；或者

通过社交操作系统平台，向继承人好友个人安全内核节点发送公钥获取请求，所述公钥获取请求包括用户指定的继承人个人安全内核节点标识，从继承人好友个人安全内核节点，接收用户指定的继承人个人安全内核节点标识的继承人个人安全内核节点的公钥。

17、根据权利要求 14 所述的方法，所述获取增加的数字资产凭证对应的继承人个人安全内核节点标识，以及所述继承人个人安全内核节点标识的继承人个人安全内核

节点的公钥，包括：

根据所述遗嘱中为已有的数字资产凭证指定的继承人个人安全内核节点标识，确定增加的数字资产凭证对应的继承人个人安全内核节点标识；

获取增加的数字资产凭证对应的继承人个人安全内核节点标识的继承人个人安全内核节点的公钥。

18、根据权利要求 17 所述的方法，所述根据所述遗嘱中为已有的数字资产凭证指定的继承人个人安全内核节点标识，确定增加的数字资产凭证对应的继承人个人安全内核节点标识，包括：

获取增加的数字资产凭证的类型；

查找所述遗嘱中已为相同类型的数字资产凭证指定的继承人个人安全内核节点标识；

如果遗嘱中已为相同类型的数字资产凭证指定的继承人个人安全内核节点标识一致，则将遗嘱中已为相同类型的数字资产凭证指定的继承人个人安全内核节点标识确定为增加的数字资产凭证对应的继承人个人安全内核节点标识。

19、根据权利要求 18 所述的方法，所述根据所述遗嘱中为已有的数字资产凭证指定的继承人个人安全内核节点标识，确定增加的数字资产凭证对应的继承人个人安全内核节点标识，还包括：

如果遗嘱中已为相同类型的数字资产凭证指定的继承人个人安全内核节点标识不一致，则将遗嘱中已为相同类型的数字资产凭证指定的多个继承人个人安全内核节点标识中最多的继承人个人安全内核节点标识，确定为增加的数字资产凭证对应的继承人个人安全内核节点标识。

20、根据权利要求 17 所述的方法，所述根据所述遗嘱中为已有的数字资产凭证指定的继承人个人安全内核节点标识，确定增加的数字资产凭证对应的继承人个人安全内核节点标识，包括：

获取增加的数字资产凭证的业务依赖方节点标识；

查找所述遗嘱中已为相同业务依赖方节点标识的数字资产凭证指定的继承人个人安全内核节点标识；

如果遗嘱中已为相同业务依赖方节点标识的数字资产凭证指定的继承人个人安全内核节点标识一致，则将遗嘱中已为相同业务依赖方节点标识的数字资产凭证指定的继承人个人安全内核节点标识确定为增加的数字资产凭证对应的继承人个人安全内核节点标识。

21、根据权利要求 20 所述的方法，所述根据所述遗嘱中为已有的数字资产凭证指定的继承人个人安全内核节点标识，确定增加的数字资产凭证对应的继承人个人安全内核节点标识，还包括：

如果所述遗嘱中已为相同业务依赖方节点标识的数字资产凭证指定的继承人个人安全内核节点标识不一致，则将遗嘱中已为相同业务依赖方节点标识的数字资产凭证指定的多个继承人个人安全内核节点标识中最多的继承人个人安全内核节点标识，确定为增加的数字资产凭证对应的继承人个人安全内核节点标识。

22、根据权利要求 14 至 21 中任一项所述的方法，所述对增加的数字资产凭证，用所述继承人个人安全内核节点的公钥进行签名，包括：

按照预定的摘要算法生成增加的数字资产凭证的摘要；

用所述继承人个人安全内核节点的公钥对所述增加的数字资产凭证的摘要进行加密。

23、一种司法机构节点，包括：

获取单元，用于当用户的个人安全内核节点中增加数字资产凭证时，获取增加的数字资产凭证对应的继承人个人安全内核节点标识，以及所述继承人个人安全内核节点标识的继承人个人安全内核节点的公钥；

第一签名处理单元，用于对增加的数字资产凭证，用所述继承人个人安全内核节

点的公钥进行签名，得到增加的数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名；

添加单元，用于将所述继承人个人安全内核节点标识、增加的数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名，添加到所述用户的遗嘱中，所述遗嘱中包含有用司法机构节点公钥进行的签名；

第二签名处理单元，用于将所述遗嘱中包含的用司法机构节点公钥进行的签名去掉，将所述遗嘱中的当前内容用所述司法机构节点公钥进行签名，并将得到的签名放入所述遗嘱。

24、一种司法机构节点，包括：

存储器，存储有计算机可读指令；

处理器，读取存储器存储的计算机可读指令，以执行权利要求 1-12 中的任一个所述的方法、或者权利要求 14-22 中的任一个所述的方法。

25、一种计算机程序介质，其上存储有计算机可读指令，当所述计算机可读指令被计算机的处理器执行时，使计算机执行权利要求 1-12 中的任一个所述的方法、或者权利要求 14-22 中的任一个所述的方法。

26、一种包括指令的计算机程序产品，当其在计算机上运行时，使得所述计算机执行权利要求 1-12 中的任一个所述的方法、或者权利要求 14-22 中的任一个所述的方法。

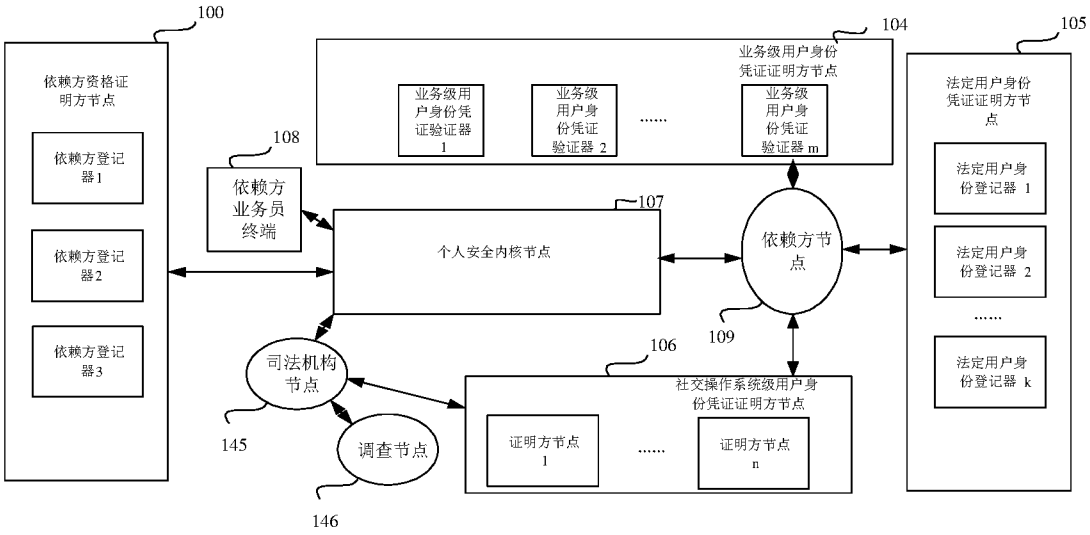
100
依赖方资格证明方节点
依赖方登记器1
依赖方登记器2
依赖方登记器3
104
业务级用户身份凭证证明方节点
业务级用户身份凭证验证器1
业务级用户身份凭证验证器2
.....
业务级用户身份凭证验证器m
105
法定用户身份凭证证明方节点
法定用户身份登记器1
法定用户身份登记器2
.....
法定用户身份登记器k
108
依赖方业务员终端
107
个人安全内核节点
依赖方节点
109
106
社交操作系统级用户身份凭证证明方节点
证明方节点1
.....
证明方节点n
司法机构节点
145
调查节点
146

图 1A

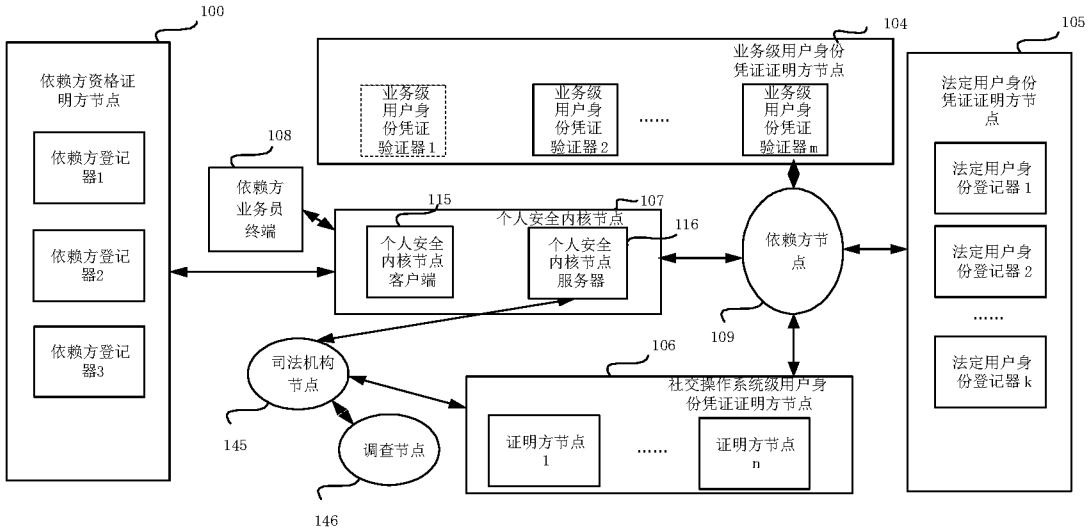
100
依赖方资格证明方节点
依赖方登记器1
依赖方登记器2
依赖方登记器3
104
业务级用户身份凭证证明方节点
业务级用户身份凭证验证器1
业务级用户身份凭证验证器2
.....
业务级用户身份凭证验证器m
105
法定用户身份凭证证明方节点
法定用户身份登记器1
法定用户身份登记器2
.....
法定用户身份登记器k
108
依赖方业务员终端
115
个人安全内核节点客户端
107
个人安全内核节点
个人安全内核节点服务器
116
依赖方节点
109
106
社交操作系统级用户身份凭证证明方节点
证明方节点1
.....
证明方节点n
司法机构节点
145
调查节点
146

图 1B

图 2A

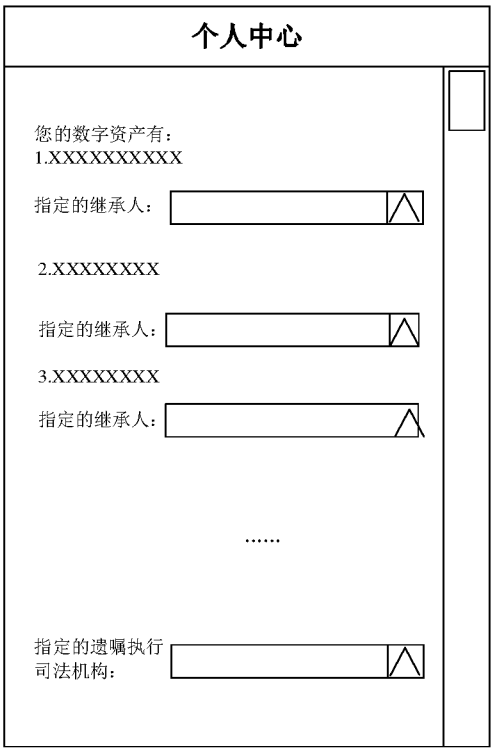

图 2B

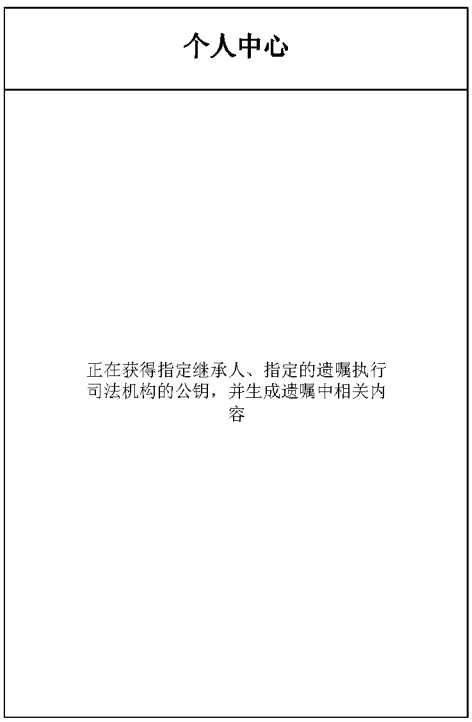

图 2C

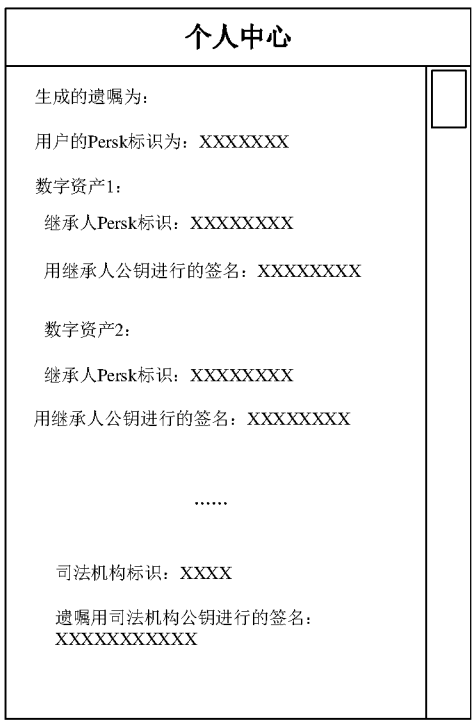

图 2D


个人中心
正在将生成的遗嘱记录到区块链上

图 2E

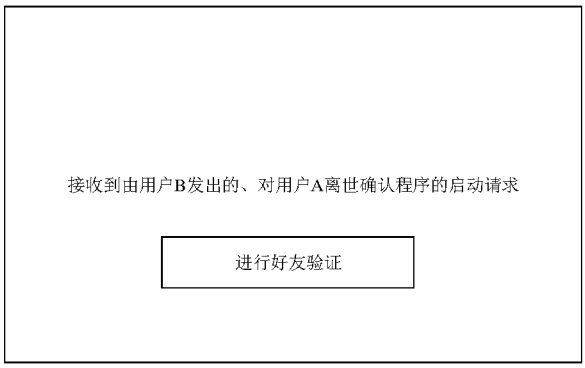
接收到由用户B发出的、对用户A离世确认程序的启动请求
进行好友验证

图 2F

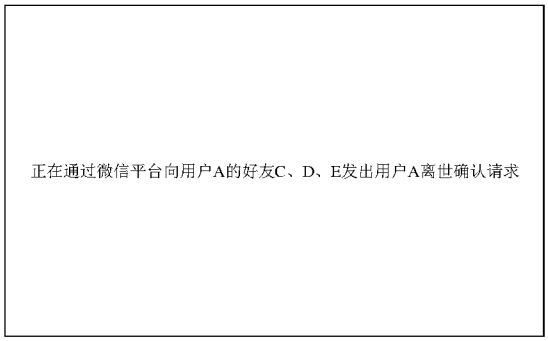

图 2G

图 2H

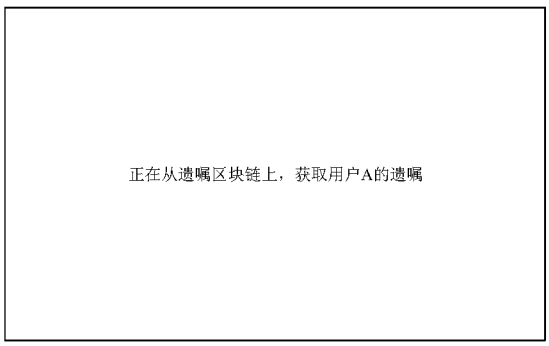

图 2I

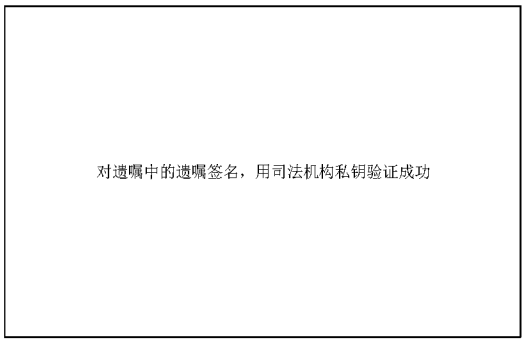

图 2J

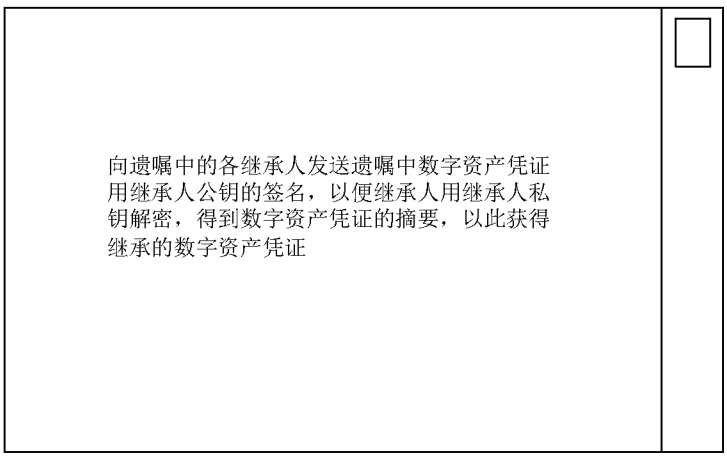

图 2K

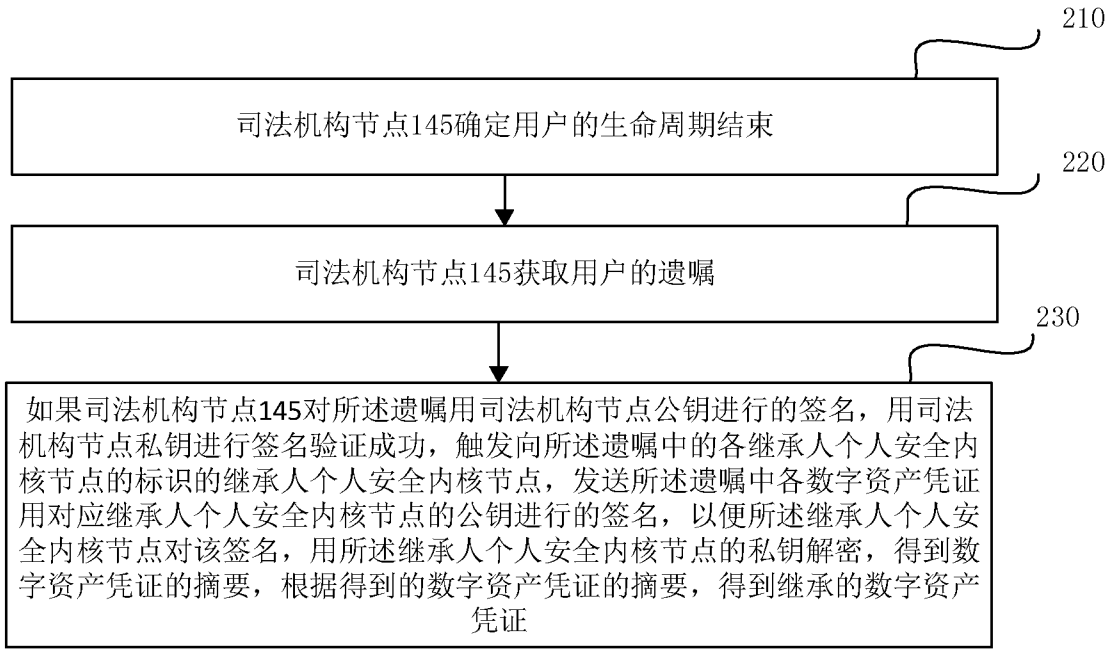
210
司法机构节点145确定用户的生命周期结束
220
司法机构节点145获取用户的遗嘱
230
如果司法机构节点145对所述遗嘱用司法机构节点公钥进行的签名，用司法机构节点私钥进行签名验证成功，触发向所述遗嘱中的各继承人个人安全内核节点的标识的继承人个人安全内核节点，发送所述遗嘱中各数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名，以便所述继承人个人安全内核节点对该签名，用所述继承人个人安全内核节点的私钥解密，得到数字资产凭证的摘要，根据得到的数字资产凭证的摘要，得到继承的数字资产凭证

图 3

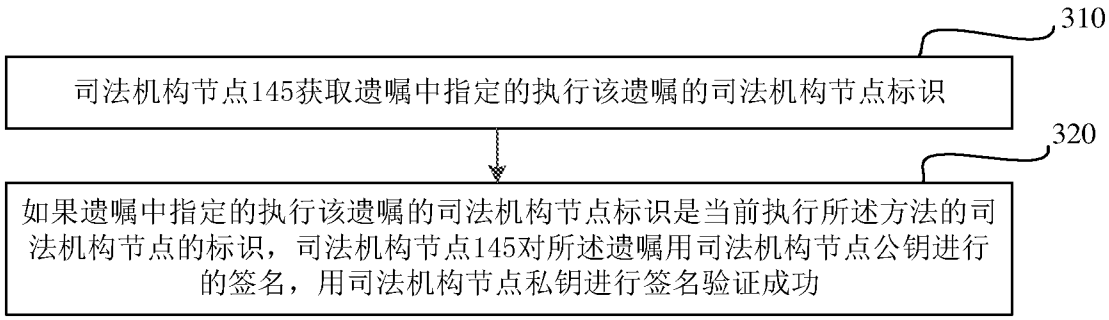
310
司法机构节点145获取遗嘱中指定的执行该遗嘱的司法机构节点标识
320
如果遗嘱中指定的执行该遗嘱的司法机构节点标识是当前执行所述方法的司法机构节点的标识，司法机构节点145对所述遗嘱用司法机构节点公钥进行的签名，用司法机构节点私钥进行签名验证成功

图 4

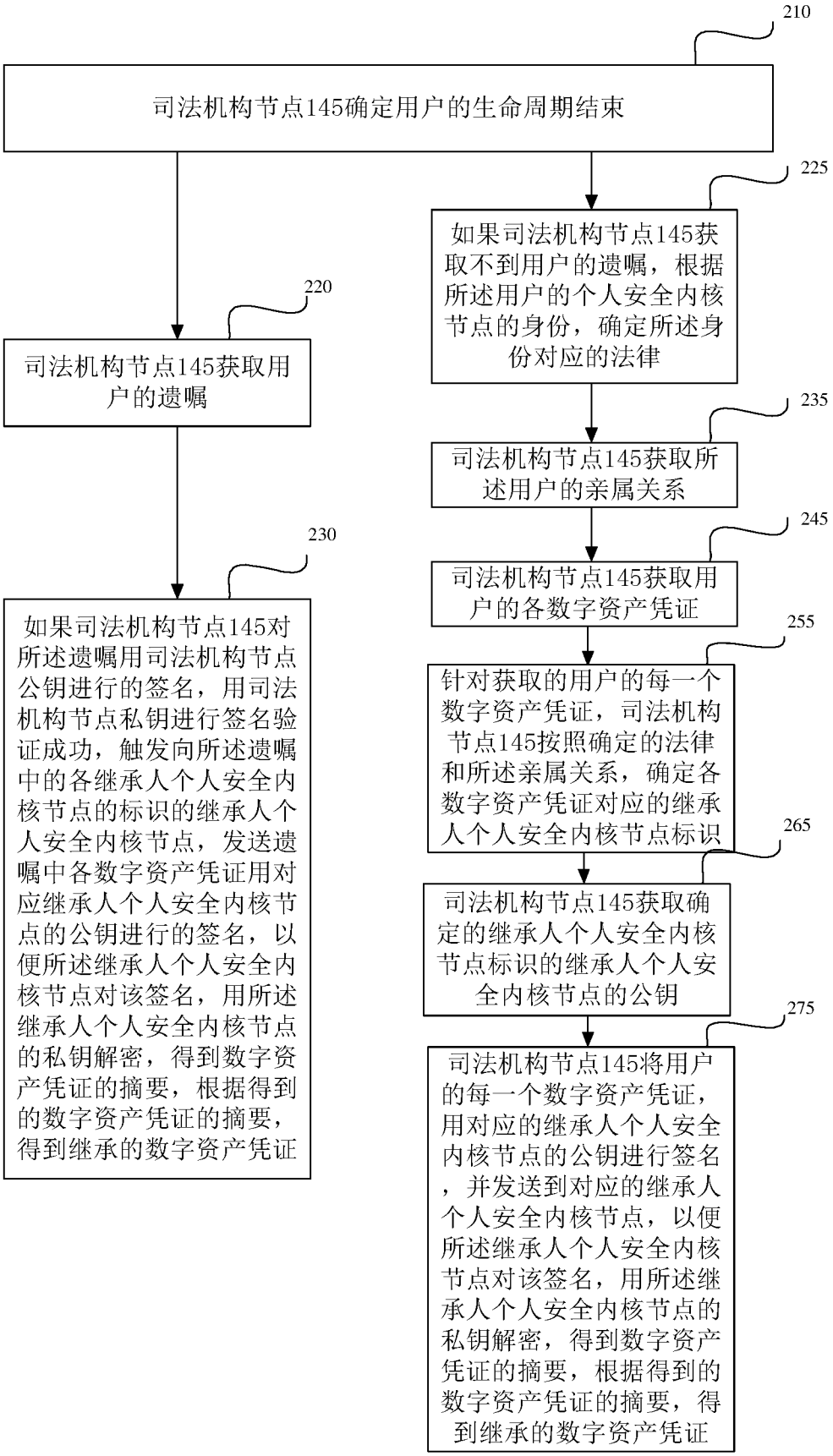
210
司法机构节点145确定用户的生命周期结束
220
司法机构节点145获取用户的遗嘱
230
如果司法机构节点145对所述遗嘱用司法机构节点公钥进行的签名，用司法机构节点私钥进行签名验证成功，触发向所述遗嘱中的各继承人个人安全内核节点的标识的继承人个人安全内核节点，发送遗嘱中各数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名，以便所述继承人个人安全内核节点对该签名，用所述继承人个人安全内核节点的私钥解密，得到数字资产凭证的摘要，根据得到的数字资产凭证的摘要，得到继承的数字资产凭证
225
如果司法机构节点145获取不到用户的遗嘱，根据所述用户的个人安全内核节点的身份，确定所述身份对应的法律
235
司法机构节点145获取所述用户的亲属关系
245
司法机构节点145获取用户的各数字资产凭证
255
针对获取的用户的每一个数字资产凭证，司法机构节点145按照确定的法律和所述亲属关系，确定各数字资产凭证对应的继承人个人安全内核节点标识
265
司法机构节点145获取确定的继承人个人安全内核节点标识的继承人个人安全内核节点的公钥
275
司法机构节点145将用户的每一个数字资产凭证，用对应的继承人个人安全内核节点的公钥进行签名，并发送到对应的继承人个人安全内核节点，以便所述继承人个人安全内核节点对该签名，用所述继承人个人安全内核节点的私钥解密，得到数字资产凭证的摘要，根据得到的数字资产凭证的摘要，得到继承的数字资产凭证

图 5

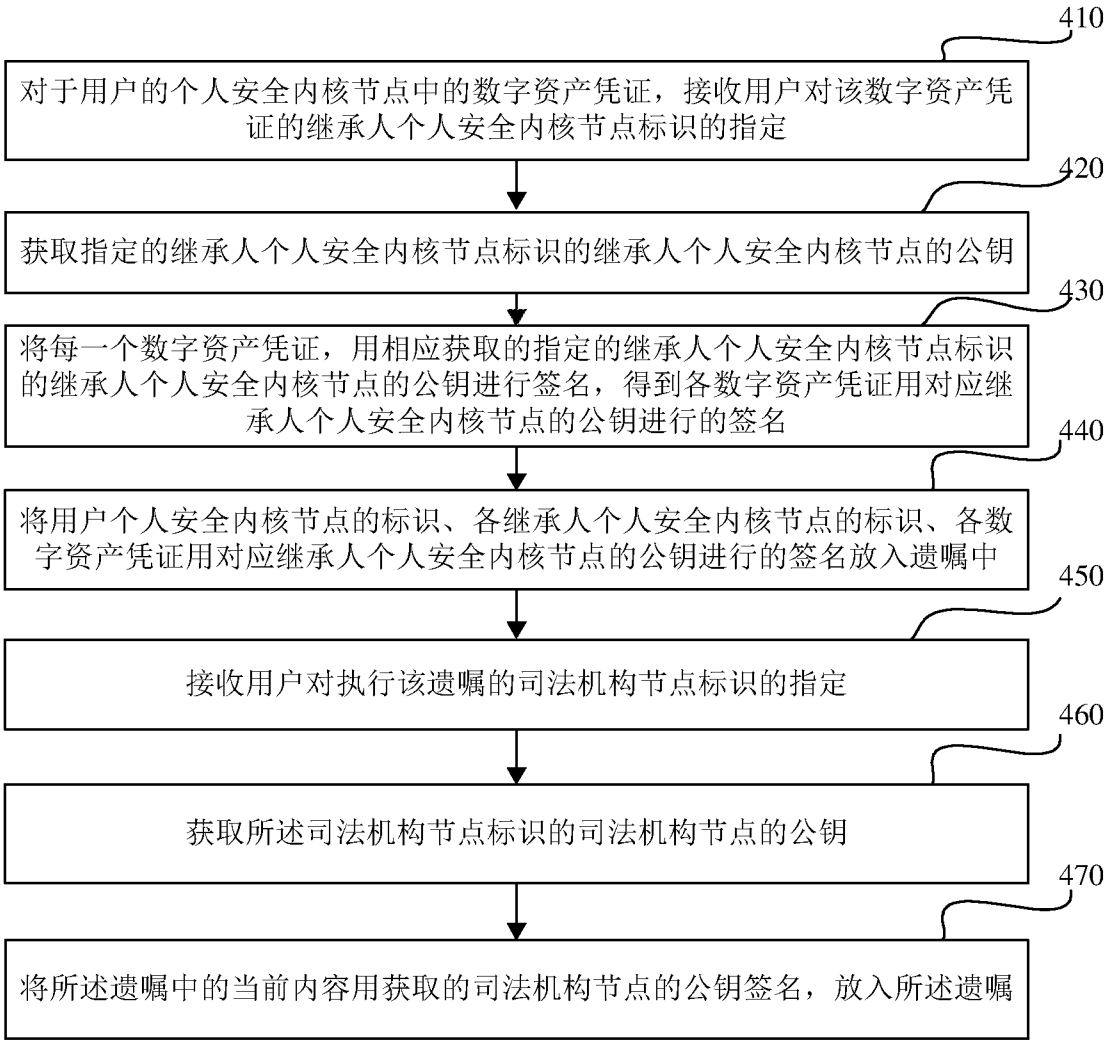
410
对于用户的个人安全内核节点中的数字资产凭证，接收用户对该数字资产凭证的继承人个人安全内核节点标识的指定
420
获取指定的继承人个人安全内核节点标识的继承人个人安全内核节点的公钥
430
将每一个数字资产凭证，用相应获取的指定的继承人个人安全内核节点标识的继承人个人安全内核节点的公钥进行签名，得到各数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名
440
将用户个人安全内核节点的标识、各继承人个人安全内核节点的标识、各数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名放入遗嘱中
450
接收用户对执行该遗嘱的司法机构节点标识的指定
460
获取所述司法机构节点标识的司法机构节点的公钥
470
将所述遗嘱中的当前内容用获取的司法机构节点的公钥签名，放入所述遗嘱

图 6

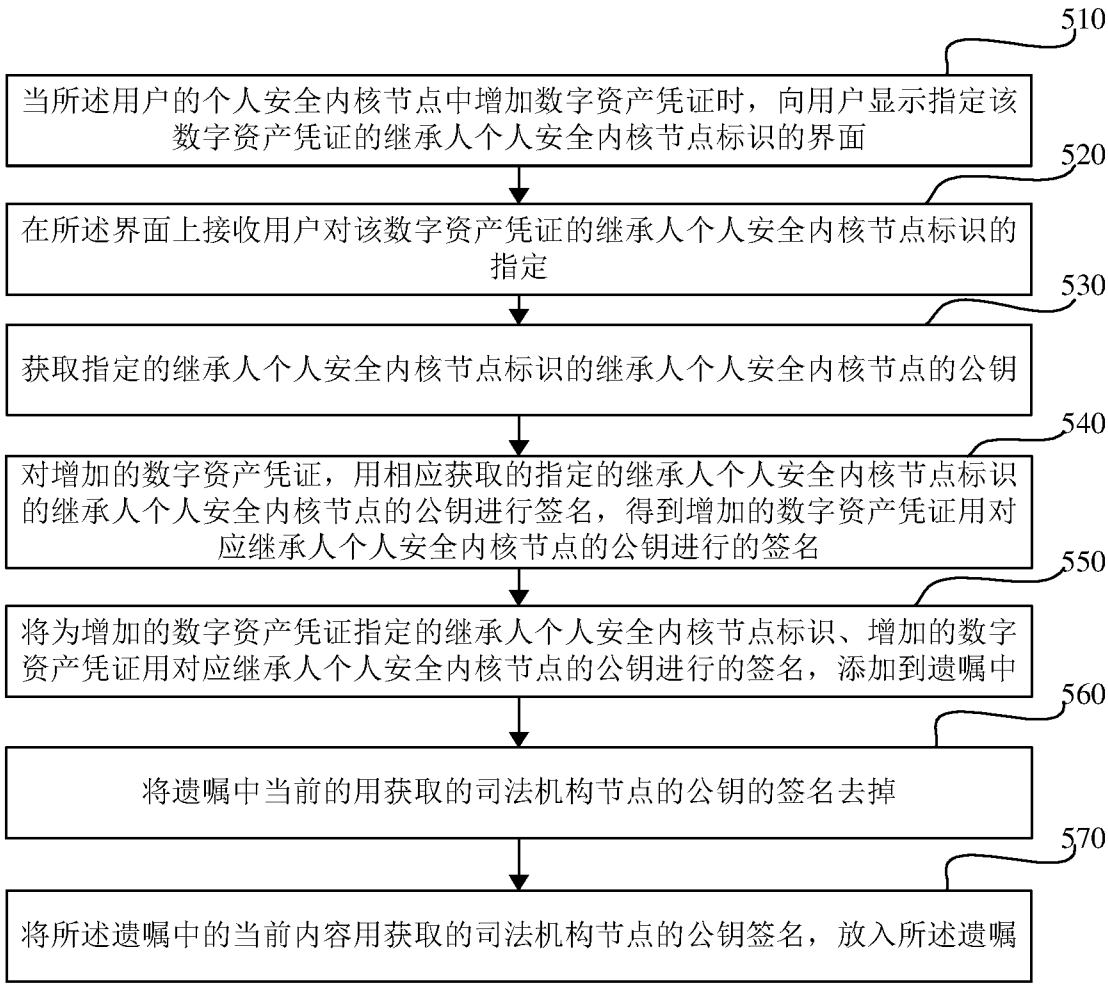
510
当所述用户的个人安全内核节点中增加数字资产凭证时，向用户显示指定该数字资产凭证的继承人个人安全内核节点标识的界面
520
在所述界面上接收用户对该数字资产凭证的继承人个人安全内核节点标识的指定
530
获取指定的继承人个人安全内核节点标识的继承人个人安全内核节点的公钥
540
对增加的数字资产凭证，用相应获取的指定的继承人个人安全内核节点标识的继承人个人安全内核节点的公钥进行签名，得到增加的数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名
550
将为增加的数字资产凭证指定的继承人个人安全内核节点标识、增加的数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名，添加到遗嘱中
560
将遗嘱中当前的用获取的司法机构节点的公钥的签名去掉
570
将所述遗嘱中的当前内容用获取的司法机构节点的公钥签名，放入所述遗嘱

图 7

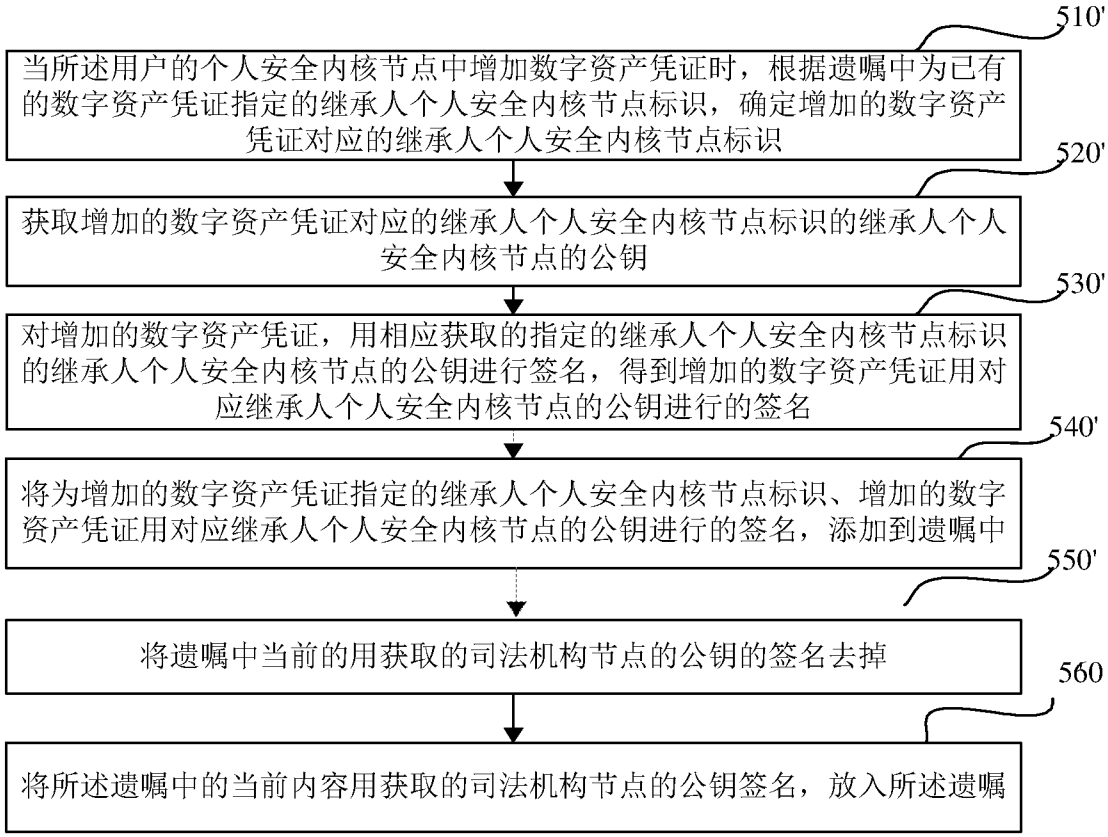
510'
当所述用户的个人安全内核节点中增加数字资产凭证时，根据遗嘱中为已有的数字资产凭证指定的继承人个人安全内核节点标识，确定增加的数字资产凭证对应的继承人个人安全内核节点标识
520'
获取增加的数字资产凭证对应的继承人个人安全内核节点标识的继承人个人安全内核节点的公钥
530'
对增加的数字资产凭证，用相应获取的指定的继承人个人安全内核节点标识的继承人个人安全内核节点的公钥进行签名，得到增加的数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名
540'
将为增加的数字资产凭证指定的继承人个人安全内核节点标识、增加的数字资产凭证用对应继承人个人安全内核节点的公钥进行的签名，添加到遗嘱中
550'
将遗嘱中当前的用获取的司法机构节点的公钥的签名去掉
560
将所述遗嘱中的当前内容用获取的司法机构节点的公钥签名，放入所述遗嘱

图 8

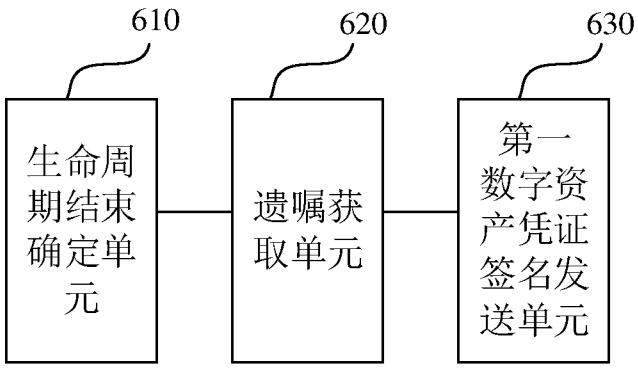
610
620
630
生命周期结束确定单元
遗嘱获取单元
第一数字资产凭证签名发送单元

图 9

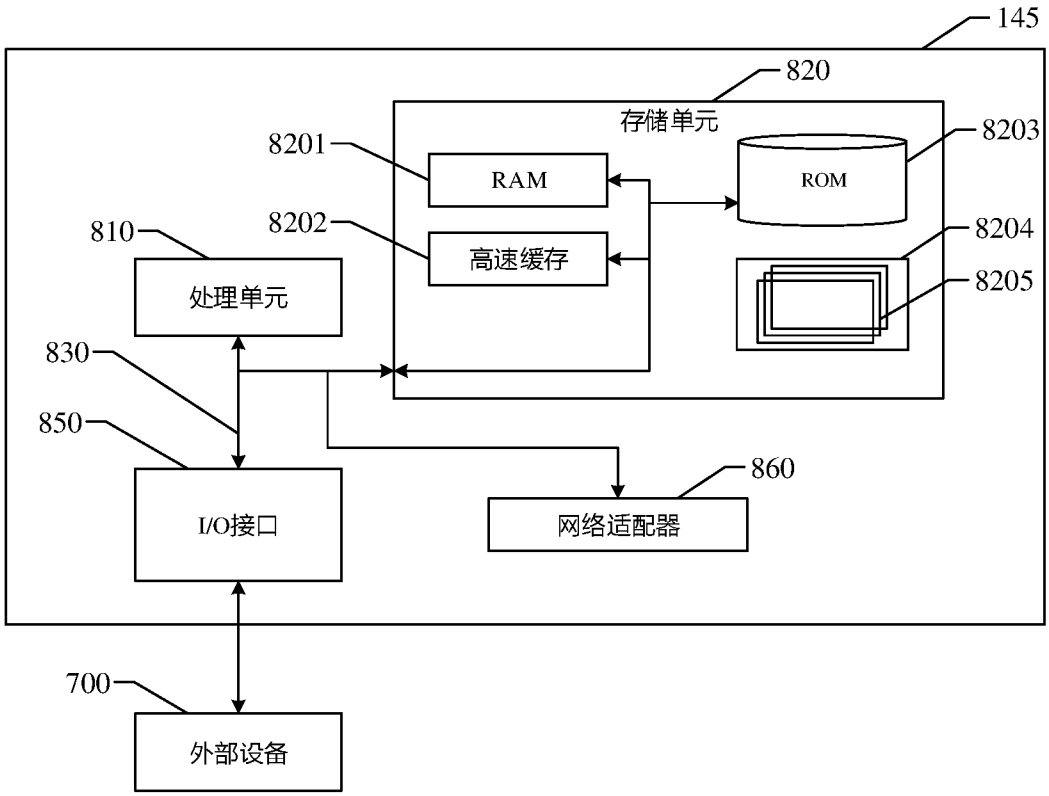
145
820
存储单元
8201
RAM
8203
ROM
8202
高速缓存
8204
8205
810
处理单元
830
850
860
I/O接口
网络适配器
700
外部设备

图 10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2020/077388

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/38(2012.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, WPI, EPODOC, CNKI, IEEE: 数字资产, 继承, 转移, 遗嘱, 生命周期, 继承, 签名, 公钥, 私钥, digital asset?, inherit, transfer, testament, life period, inherit, signature, public key, private key

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110245940 A (TENCENT TECHNOLOGY SHENZHEN CO., LTD.) 17 September 2019 (2019-09-17) claims 1-15, description, paragraphs [0004]-[0017] and [0033]-[0368], and figures 1A-10	1-26
PX	CN 110766405 A (TENCENT TECHNOLOGY SHENZHEN CO., LTD.) 07 February 2020 (2020-02-07) claims 1-12, description, paragraphs [0005]-[0021] and [0037]-[0370], and figures 1A-10	1-26
X	CN 108809630 A (ZHONGCHAO CREDITCARD INDUSTRY DEVELOPMENT CO., LTD. HANGZHOU BLOCKCHAIN TECHNOLOGY RESEARCH INSTITUTE) 13 November 2018 (2018-11-13) description, paragraphs [0005]-[0041] and [0049]-[0128], and figures 1-5	1-26
A	CN 105809062 A (BUBI TECHNOLOGIES CO., LTD.) 27 July 2016 (2016-07-27) entire document	1-26
A	CN 109345259 A (TENCENT TECHNOLOGY SHENZHEN CO., LTD.) 15 February 2019 (2019-02-15) entire document	1-26

☑ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 May 2020	**02 June 2020**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration (ISA/CN) **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2020/077388

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 109063084 A (ANHUI WENFA INFORMATION TECHNOLOGY CO., LTD.) 21 December 2018 (2018-12-21) entire document	1-26

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2020/077388

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 110245940 A	17 September 2019	None	
CN 110766405 A	07 February 2020	None	
CN 108809630 A	13 November 2018	None	
CN 105809062 A	27 July 2016	None	
CN 109345259 A	15 February 2019	None	
CN 109063084 A	21 December 2018	None	

国际检索报告

国际申请号
PCT/CN2020/077388

A. 主题的分类

G06Q 20/38(2012.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

G06Q

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNPAT,WPI,EPODOC,CNKI,IEEE: 数字资产，继承，转移，遗嘱，生命周期，继承，签名，公钥，私钥，digital asset?, inherit, transfer, testament, life period, inherit, signature, public key, private key

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
PX	CN 110245940 A (腾讯科技深圳有限公司) 2019年 9月 17日 (2019-09-17) 权利要求1-15，说明书第[0004]-[0017],[0033]-[0368]段及附图1A-10	1-26
PX	CN 110766405 A (腾讯科技深圳有限公司) 2020年 2月 7日 (2020-02-07) 权利要求1-12，说明书第[0005]-[0021]段，[0037]-[0370]及附图1A-10	1-26
X	CN 108809630 A (中钞信用卡产业发展有限公司杭州区块链技术研究院) 2018年 11月 13日 (2018-11-13) 说明书第[0005]-[0041]、[0049]-[0128]段及附图1-5	1-26
A	CN 105809062 A (布比北京网络技术有限公司) 2016年 7月 27日 (2016-07-27) 全文	1-26
A	CN 109345259 A (腾讯科技深圳有限公司) 2019年 2月 15日 (2019-02-15) 全文	1-26
A	CN 109063084 A (安徽问法信息技术有限公司) 2018年 12月 21日 (2018-12-21) 全文	1-26

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2020年 5月 16日	2020年 6月 2日
ISA/CN的名称和邮寄地址 中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 王晓飞 电话号码 86-(10)-53961389

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2020/077388

检索报告引用的专利文件	公布日 (年/月/日)	同族专利	公布日 (年/月/日)
CN 110245940 A	2019年 9月 17日	无	
CN 110766405 A	2020年 2月 7日	无	
CN 108809630 A	2018年 11月 13日	无	
CN 105809062 A	2016年 7月 27日	无	
CN 109345259 A	2019年 2月 15日	无	
CN 109063084 A	2018年 12月 21日	无	