(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 7 月 30 日 (30.07.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/151322 A1

(51) 国际专利分类号:
G06F 21/32 (2013.01) *H04L 29/06* (2006.01)

(21) 国际申请号: PCT/CN2019/117804

(22) 国际申请日: 2019 年 11 月 13 日 (13.11.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910060458.9 2019年1月22日 (22.01.2019) CN

(71) 申请人: 平安科技（深圳）有限公司 (PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) [CN/CN]; 中国广东省深圳市福田区福田街道福安社区益田路5033号平安金融中心23楼, Guangdong 518033 (CN)。

(72) 发明人: 胡静远 (HU, Jingyuan); 中国广东省深圳市福田区福田街道福安社区益田路5033号平安金融中心23楼, Guangdong 518033 (CN)。

(74) 代理人: 北京鸿元知识产权代理有限公司 (GRANDER IP LAW FIRM); 中国北京市朝阳区光华路7号汉威大厦东区18A6室, Beijing 100004 (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,

WO 2020/151322 A1

(54) **Title:** IDENTITY MANAGEMENT METHOD, APPARATUS AND DEVICE BASED ON BLOCKCHAIN, AND STORAGE MEDIUM

(54) 发明名称: 基于区块链的身份管理方法、装置、设备及存储介质

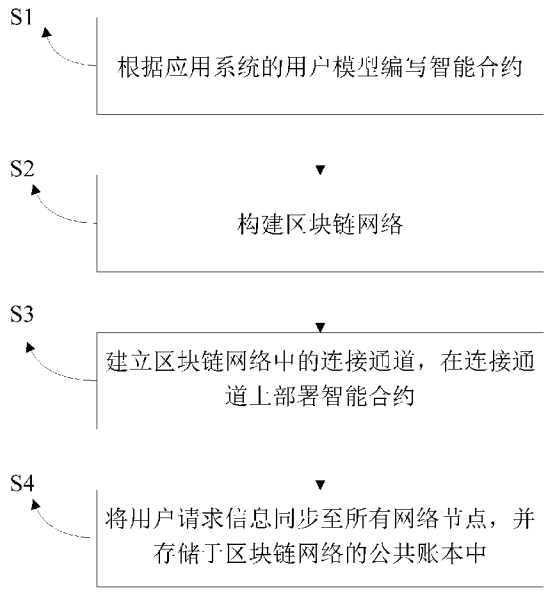

图 1

(57) **Abstract:** The present application falls within the technical field of blockchains, and disclosed are an identity management method, apparatus and device based on a blockchain, and a storage medium. The method comprises: respectively writing intelligent contracts according to user models of an application system; constructing a blockchain network, wherein the blockchain network comprises a plurality of network nodes, a plurality of application systems, and a public account book; and each application system corresponds to at least one network node, and each network node automatically synchronizes blockchain data by means of a consensus mechanism;

[见续页]

PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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))。

establishing a connection channel between each application system in the blockchain network, and deploying an intelligent contract on the connection channels; receiving a user request by means of the application system, and calling a corresponding intelligent contract according to the user request; and synchronizing user request information to all the network nodes by means of the connection channels, and storing same in the public account book of the blockchain network. By means of the electronic device of the present application, the user request information does not need to be fully redirected to a centralized server, and security reliability is relatively high.

(57) 摘要：本申请属于区块链技术领域, 公开了一种基于区块链的身份管理方法, 装置, 设备及存储介质, 所述方法包括: 根据应用系统的用户模型分别编写智能合约; 构建区块链网络, 所述区块链网络包括多个网络节点, 多个应用系统和公共账本, 每个应用系统均对应至少一个网络节点, 各个网络节点通过共识机制自动同步区块链数据; 建立所述区块链网络中各个应用系统之间的连接通道, 在所述连接通道上部署智能合约; 通过应用系统接收用户请求, 根据所述用户请求调用相应的智能合约, 将用户请求信息通过所述连接通道同步至所有网络节点, 存储于所述区块链网络的公共账本中. 电子设备本申请用户请求信息不必再全部重定向至中心化服务器, 安全可靠性较高.

基于区块链的身份管理方法、装置、设备及存储介质

本申请要求于 2019 年 01 月 22 日提交的中国专利申请号 201910060458.9 的优先权益，上述案件全部内容以引用的方式并入本文中。

技术领域

本申请涉及区块链技术领域，尤其涉及一种基于区块链的身份管理方法、装置、设备及存储介质。

背景技术

企业在信息化的过程中会根据不同阶段的需求构建多种信息系统，当不同的信息系统中包含独立的用户管理模块，同一个用户使用不同的应用系统时，由于用户模型的不同，导致存储方式差异性，增加了各应用系统之间用户信息同步的复杂性和系统维护成本，各个应用系统之间相互独立、数据不一致、信息共享程度不高，使得对用户的身份管理较为麻烦。现有解决方式是采用单点登录的方式构建统一用户管理系统。单点登录的实质就是当客户端输入用户名密码向某应用服务器发起请求时，该应用服务器将重定向到单点登录（SSO，Single Sign On）服务器进行身份验证，产生身份凭证，并将带有身份凭证的请求重定向至被请求的应用服务器，由应用服务器从凭证中提取出用户的身份信息。由于所有的请求都重定向至SSO服务器，这种中心化的方式会增加SSO服务器的压力，并且SSO服务器生成的身份凭证在各应用系统传递的过程中存在安全问题。

发明内容

本申请提供一种基于区块链的身份管理方法、装置、设备及存储介质，以解决现有技术中单点登录方式易增加SSO服务器的压力，并且身份凭证在传递过程中存在安全隐患的问题。

为了实现上述目的，本申请的第一个方面是提供一种基于区块链的身份管理方法，包括：

根据应用系统的用户模型分别编写智能合约；

构建区块链网络，所述区块链网络包括多个网络节点、多个应用系统和公共账本，每个应用系统均对应至少一个网络节点，各个网络节点通过共识机制自动同步区块链数据；

建立所述区块链网络中各个应用系统之间的连接通道，在所述连接通道上部署智能合约；

通过应用系统接收用户请求，根据所述用户请求调用相应的智能合约，将用户请求信息通过所述连接通道同步至所有网络节点，存储于所述区块链网络的公共账本中。

为了实现上述目的，本申请的第二个方面是提供一种基于区块链的身份管理装置，包括：

合约生成模块，用于根据应用系统的用户模型分别编写智能合约；

区块链构建模块，用于构建区块链网络，所述区块链网络包括多个网络节点、多个应用系统和公共账本，每个应用系统均对应至少一个网络节点，各个网络节点通过共识机制自动同步区块链数据；

通道建立模块，用于建立所述区块链网络中各个应用系统之间的连接通道，在所述连接通道上部署智能合约；

存储模块，用于通过应用系统接收用户请求，根据所述用户请求调用相应的智能合约，将用户请求信息通过所述连接通道同步至所有网络节点，存储于所述区块链网络的公共账本中。

为了实现上述目的，本申请的第三个方面是提供一种电子设备，该电子设备包括：

处理器和存储器，所述存储器中包括基于区块链的身份管理程序，所述基于区块链的身份管理程序被所述处理器执行时实现如上所述的基于区块链的身份管理方法。

为了实现上述目的，本申请的第四个方面是提供一种计算机非易失性可读存储介质，所述计算机非易失性可读存储介质中包括基于区块链的身份管理程序，所述基于区块链的身份管理程序被处理器执行时，实现如上所述的基于区块链的身份管理方法。

相对于现有技术，本申请具有以下优点和有益效果：

本申请通过构建的区块链网络对多个应用系统进行整合，根据区块链去

中心化的特性，使得一个应用系统的数据可以在区块链网络中的多个应用系统之间共享，每个应用系统只需要调用相应的本地智能合约，即可将用户请求信息写入区块链中，而用户请求不必再全部重定向至中心化服务器。并且，根据区块链去信任的特性，通过区块链网络可以保证用户信息在各个网络节点之间安全有效地同步。根据区块链不可篡改的特性，保障写入信息的可靠性。

附图说明

图1为本申请所述基于区块链的身份管理方法的流程示意图；

图2为本申请中区块链网络结构示意图；

图3为本申请中基于区块链的身份管理装置的示意图。

本申请目的的实现、功能特点及优点将结合实施例，参照附图做进一步说明。

具体实施方式

下面将参考附图来描述本申请所述的实施例。本领域的普通技术人员可以认识到，在不偏离本申请的精神和范围的情况下，可以用各种不同的方式或其组合对所描述的实施例进行修正。因此，附图和描述在本质上是说明性的，仅仅用以解释本申请，而不是用于限制权利要求的保护范围。此外，在本说明书中，附图未按比例画出，并且相同的附图标记表示相同的部分。

由于不同应用系统中包含不同的用户模型，通过用户模型存储用户信息时，因用户模型的不同导致各用户信息之间的同步更加复杂，本申请所述基于区块链的身份管理方法，旨在对多个应用系统的信息进行整合，将用户信息写入区块链网络中，以保证用户信息在各个应用系统之间的同步性，当用户在多个应用系统登录时，通过区块链网络对用户信息进行验证。图 1 为本申请所述基于区块链的身份管理方法的流程示意图，如图 1 所示，所述身份管理方法包括：

步骤 S1、根据应用系统的用户模型分别编写智能合约；

步骤 S2、构建区块链网络，如图 2 所示，所述区块链网络包括多个网络节点、多个应用系统和公共账本，每个应用系统均对应至少一个网络节点，

各个网络节点通过共识机制自动同步区块链数据；

步骤 S3、建立所述区块链网络中各个应用系统之间的连接通道，在所述连接通道上部署智能合约；

步骤 S4、通过应用系统接收用户请求，根据所述用户请求调用相应的智能合约，将用户请求信息通过所述连接通道同步至所有网络节点，存储于所述区块链网络的公共账本中。

本申请通过构建的区块链网络对多个应用系统进行整合，区块链网络中的数据可以在链上的多个应用系统之间共享，每个应用系统只需要调用相应的本地智能合约，即可将用户请求信息写入区块链中，而用户请求不必再全部重定向至中心化服务器。并且，通过区块链网络可以保证用户信息在各个网络节点之间安全有效地同步，并保证写入信息的可靠性。每个应用系统均有各自的网络节点，有效缓解 SSO 服务器的压力。

本申请中，应用系统指的是企业根据不同阶段的需求构建的信息系统，每个应用系统具有不同的用户模型。例如，应用系统可以是产险系统、车险系统和银行系统等。不同的用户模型包括不同的用户信息，例如，车险系统的用户模型包括用户信息、车辆信息、车险信息等，银行系统的用户模型包括用户的身份信息、银行卡信息、信用卡额度信息、银行卡余额信息等。用户请求包括用户注册、用户信息验证、用户登录、用户交易以及用户对应用系统中用户信息的增加、修改、完善和查询等。

本申请中，智能合约根据应用系统的用户模型编写，智能合约上编写业务函数，实现不同的功能，并且将智能合约部署于区块链的网络节点间，使其不可篡改，保障通过智能合约写入信息的可靠性。优选地，所述智能合约包括用户注册模块、用户验证模块、登录凭证获取模块、声纹录入模块、指纹录入模块和人脸识别图像录入模块中的一种或多种。不同的应用系统所编写的智能合约不同，应用系统根据用户请求调用相应的智能合约，从相应的智能合约中选择相应的模块，实现相应的功能。例如，当应用系统上有新用户注册时，应用系统接收该用户的注册请求，根据用户的注册请求调用与该应用系统对应的本地智能合约中的用户注册模块，写入用户的注册信息，通过区块链网络的连接通道将该用户的注册信息共享至其他的应用系统，使得该用户在其他应用系统可以直接登录，而无需再次注册。

本申请的一个实施例中，将用户请求信息通过所述连接通道同步至所有网络节点的步骤之后，还包括：通过应用系统接收用户的登录请求，应用系统通过调用对应的智能合约，匹配用户的登录信息与所述公共账本中存储的注册信息，若匹配成功，则用户在所述应用系统中有登录权限，若匹配失败，则用户在所述应用系统中没有登录权限，需要重新注册，从而实现对用户身份的验证。进一步地，通过应用系统接收用户的登录请求的步骤之前，还包括：通过应用系统接收用户的注册请求，应用系统通过调用对应的智能合约，将所述注册请求对应的注册信息写入所述区块链网络，存储于所述公共账本中。接收用户的登录请求和注册请求的应用系统可以是同一个应用系统，也可以是不同的应用系统。

本申请的一个实施例中，根据所述用户请求调用相应的智能合约的步骤包括：响应所述用户请求；通过封装的 java-sdk 调用与所述用户请求对应的智能合约。

优选地，所述区块链网络还包括多个私有账本，所述私有账本与所述应用系统一一对应。其中，所述私有账本用于记录所述应用系统的特有信息，且不为区块链网络中的其他应用系统共享，以保证区块链中同一个链上的各应用系统特有数据的隔离，即使在同一链中的其他应用系统，均不可读取与修改私有账本中特有的未授权信息。例如，虽然车险应用系统和产险应用系统在支付过程中会用到银行应用系统的银行卡信息和余额信息，但是对用户的信用卡额度等等的信息是不可知的，属于银行应用系统的特有信息，这类敏感信息可存放于银行应用系统的私有账本中，不会在公共账本中共享至区块链中的所有应用系统，公共账本中仅保留每个私有账本中的哈希值；若在其他应用系统中需要查看，则需要银行应用系统的授权才可以查看，授权信息会存于公共账本之上便于各组织查看。

优选地，所述基于区块链的身份管理方法还包括：根据用户信息通过编写配置文件配置控制策略，通过所述网络节点根据所述控制策略检测所述用户权限，从而确定该用户对应的用户权限以及对应用户权限可以使用的应用系统，以便于根据用户权限判断是否响应用户请求。其中，所述控制策略包括自主型访问控制策略、系统强制性访问控制策略、基于角色的访问控制策略和基于属性证书的访问控制策略等，自主型访问控制策略由用户来决定访

问控制权限，是一种基于身份的控制策略，系统强制性访问控制策略是操作系统根据限定规则决定的访问控制权限，基于属性证书的访问控制策略是将权限信息放置于用户的属性证书中，系统根据属性证书决定访问控制权限。

进一步地，通过应用系统接收用户请求的步骤之后，所述基于区块链的身份管理方法还包括：对所述用户请求进行验证，匹配所述用户请求与用户权限，若匹配成功，则通过验证，响应所述用户请求，若匹配失败，则未通过验证，拒绝所述用户请求，以响应与用户权限对应的用户请求，增强系统交易的安全可靠性。

优选地，所述基于区块链的身份管理方法还包括：通过所述网络节点共享各个应用系统的用户交易信息，以便于根据用户交易信息对用户进行聚类。例如，根据用户交易信息可以将银行应用系统的用户划分为不同类别，包括储蓄卡业务类别、信用卡业务类别等，根据类别的不同向用户推送不同的应用系统消息。

所述用户交易信息包括交易类型标识、应用系统标识、用户设备标识、用户身份标识中的一种或多种，其中，交易类型标识用于标识用户发起的交易类型（车险交易、储蓄交易等），应用系统标识用于标识用户交易所用的应用系统（车险应用系统、银行应用系统等），用户设备标识用于标识用户发起交易所使用的设备（客户端 APP、计算机终端等），用户身份标识用于标识用户在该应用系统内的身份（普通用户、VIP 用户等）。

本申请的一个实施例中，所述身份管理方法还包括：生成用户操作报表。具体地，包括：响应用户请求，记录当前用户的操作记录；将所述操作记录生成数据区块；将所述数据区块写入所述区块链网络中；对所述数据区块中的存储数据进行处理，生成当前用户的操作报表。所述操作报表包括用户的操作时间、操作类型、操作内容等，便于根据操作报表对用户行为进行统计分析。

本申请所述基于区块链的身份管理方法应用于电子设备，所述电子设备可以是电视机、智能手机、平板电脑、计算机等终端设备。

所述电子设备包括：处理器和存储器，所述存储器用于存储基于区块链的身份管理程序，处理器执行所述基于区块链的身份管理程序，实现以下的基于区块链的身份管理方法的步骤：

根据应用系统的用户模型分别编写智能合约；

构建区块链网络，所述区块链网络包括多个网络节点、多个应用系统和公共账本，每个应用系统均对应至少一个网络节点，各个网络节点通过共识机制自动同步区块链数据；

建立所述区块链网络中各个应用系统之间的连接通道，在所述连接通道上部署智能合约；

通过应用系统接收用户请求，根据所述用户请求调用相应的智能合约，将用户请求信息通过所述连接通道同步至所有网络节点，存储于所述区块链网络的公共账本中。

所述电子设备还包括网络接口和通信总线等。其中，网络接口可以包括标准的有线接口、无线接口，通信总线用于实现各个组件之间的连接通信。

存储器包括至少一种类型的可读存储介质，可以是闪存、硬盘、光盘等非易失性存储介质，也可以是插接式硬盘等，且并不限于此，可以是以非暂时性方式存储指令或软件以及任何相关联的数据文件并向处理器提供指令或软件程序以使该处理器能够执行指令或软件程序的任何装置。本申请中，存储器存储的软件程序包括基于区块链的身份管理程序，并可以向处理器提供该基于区块链的身份管理程序，以使得处理器可以执行该基于区块链的身份管理程序，实现基于区块链的身份管理方法。

处理器可以是中央处理器、微处理器或其他数据处理芯片等，可以运行存储器中的存储程序，例如，本申请中基于区块链的身份管理程序。

所述电子设备还可以包括显示器，显示器也可以称为显示屏或显示单元。在一些实施例中显示器可以是 LED 显示器、液晶显示器、触控式液晶显示器以及有机发光二极管(Organic Light-Emitting Diode，OLED)触摸器等。显示器用于显示在电子设备中处理的信息以及用于显示可视化的工作界面。

所述电子设备还可以包括用户接口，用户接口可以包括输入单元（比如键盘）、语音输出装置（比如音响、耳机）等。

需要说明的是，本申请之电子设备的具体实施方式与上述基于区块链的身份管理方法的具体实施方式大致相同，在此不再一一赘述。

图 3 为本申请中基于区块链的身份管理装置的示意图，如图 3 所示，本申请所述基于区块链的身份管理装置包括：

合约生成模块 1，用于根据应用系统的用户模型分别编写智能合约；

区块链构建模块 2，用于构建区块链网络，所述区块链网络包括多个网络节点、多个应用系统和公共账本，每个应用系统均对应至少一个网络节点，各个网络节点通过共识机制自动同步区块链数据；

通道建立模块 3，用于建立所述区块链网络中各个应用系统之间的连接通道，在所述连接通道上部署智能合约；

存储模块 4，用于通过应用系统接收用户请求，根据所述用户请求调用相应的智能合约，将用户请求信息通过所述连接通道同步至所有网络节点，存储于所述区块链网络的公共账本中。

优选地，所述智能合约包括用户注册模块、用户验证模块、登录凭证获取模块、声纹录入模块、指纹录入模块和人脸识别图像录入模块中的一种或多种。不同的应用系统所编写的智能合约不同，应用系统根据用户请求调用相应的智能合约，从相应的智能合约中选择相应的模块，实现相应的功能。例如，当应用系统上有新用户注册时，应用系统接收该用户的注册请求，根据用户的注册请求调用与该应用系统对应的本地智能合约中的用户注册模块，写入用户的注册信息，通过区块链网络的连接通道将该用户的注册信息共享至其他的应用系统，使得该用户在其他应用系统可以直接登录，而无需再次注册。

本申请的一个实施例中，所述身份管理装置在将用户请求信息通过所述连接通道同步至所有网络节点之后，还可以实现以下步骤：通过应用系统接收用户的登录请求，应用系统通过调用对应的智能合约，匹配用户的登录信息与所述公共账本中存储的注册信息，若匹配成功，则用户在所述应用系统中有登录权限，若匹配失败，则用户在所述应用系统中没有登录权限，需要重新注册。进一步地，所述身份管理装置在通过应用系统接收用户的登录请求的步骤之前，还可以实现以下步骤：通过应用系统接收用户的注册请求，应用系统通过调用对应的智能合约，将所述注册请求对应的注册信息写入所述区块链网络，存储于所述公共账本中。接收用户的登录请求和注册请求的应用系统可以是同一个应用系统，也可以是不同的应用系统。

本申请的一个实施例中，所述存储模块 4 通过下述方式根据所述用户请求调用相应的智能合约，具体的步骤包括：响应所述用户请求；通过封装的

java-sdk 调用与所述用户请求对应的智能合约。

优选地，所述区块链网络还包括多个私有账本，所述私有账本与所述应用系统一一对应。其中，所述私有账本用于记录所述应用系统的特有信息，且不为区块链网络中的其他应用系统共享，以保证区块链中同一个链上的各应用系统特有数据的隔离，即使在同一链中的其他应用系统，均不可读取与修改私有账本中特有的未授权信息。例如，虽然车险应用系统和产险应用系统在支付过程中会用到银行应用系统的银行卡信息和余额信息，但是对用户的信用卡额度等等的信息是不可知的，属于银行应用系统的特有信息，这类敏感信息可存放于银行应用系统的私有账本中，不会在公共账本中共享至区块链中的所有应用系统，公共账本中仅保留每个私有账本中的哈希值；若在其他应用系统中需要查看，则需要银行应用系统的授权才可以查看，授权信息会存于公共账本之上便于各组织查看。

优选地，所述身份管理装置还包括权限检测模块，根据用户信息通过编写配置文件配置控制策略，通过所述网络节点根据所述控制策略检测所述用户权限，从而确定该用户对应的用户权限以及对应用户权限可以使用的应用系统，以便于根据用户权限判断是否响应用户请求。

进一步地，所述身份管理装置还包括验证模块，在通过应用系统接收用户请求之后，对所述用户请求进行验证，匹配所述用户请求与用户权限，若匹配成功，则通过验证，响应所述用户请求，若匹配失败，则未通过验证，拒绝所述用户请求。

优选地，所述身份管理装置还实现以下的身份管理方法的步骤：通过所述网络节点共享各个应用系统的用户交易信息，以便于根据用户交易信息对用户进行聚类。例如，根据用户交易信息可以将银行应用系统的用户划分为不同类别，包括储蓄卡业务类别、信用卡业务类别等，根据类别的不同向用户推送不同的应用系统消息。

所述用户交易信息包括交易类型标识、应用系统标识、用户设备标识、用户身份标识等，其中，交易类型标识用于标识用户发起的交易类型（车险交易、储蓄交易等），应用系统标识用于标识用户交易所用的应用系统（车险应用系统、银行应用系统等），用户设备标识用于标识用户发起交易所使用的设备（客户端 APP、计算机终端等），用户身份标识用于标识用户在该应用系

统内的身份（普通用户、VIP 用户等）。

本申请的一个实施例中，所述身份管理装置还包括：报表生成单元，生成用户操作报表。具体地，所述报表生成单元包括：记录单元，响应用户请求，记录当前用户的操作记录；区块生成单元，将所述操作记录生成数据区块；区块写入单元，将所述数据区块写入所述区块链网络中；报表生成单元，对所述数据区块中的存储数据进行处理，生成当前用户的操作报表。所述操作报表包括用户的操作时间、操作类型、操作内容等。

在其他实施例中，基于区块链的身份管理程序还可以被分割为一个或者多个模块，一个或者多个模块被存储于存储器中，并由处理器执行，以完成本申请。本申请所称的模块是指能够完成特定功能的一系列计算机程序指令段。例如，所述基于区块链的身份管理程序可以被分割为：合约生成模块 1、区块链构建模块 2、通道建立模块 3 和存储模块 4。上述模块所实现的功能或操作步骤均与上文类似，此处不再详述。

本申请的一个实施例中，计算机非易失性可读存储介质可以是任何包含或存储程序或指令的有形介质，其中的程序可以被执行，通过存储的程序指令相关的硬件实现相应的功能。例如，计算机可读存储介质可以是计算机磁盘、硬盘、随机存取存储器、只读存储器等。本申请并不限于此，可以是以非暂时性方式存储指令或软件以及任何相关数据文件或数据结构并且可提供给处理器以使处理器执行其中的程序或指令的任何装置。所述计算机非易失性可读存储介质中包括基于区块链的身份管理程序，所述基于区块链的身份管理程序被处理器执行时，实现如下的基于区块链的身份管理方法：

根据应用系统的用户模型分别编写智能合约；

构建区块链网络，所述区块链网络包括多个网络节点、多个应用系统和公共账本，每个应用系统均对应至少一个网络节点，各个网络节点通过共识机制自动同步区块链数据；

建立所述区块链网络中各个应用系统之间的连接通道，在所述连接通道上部署智能合约；

通过应用系统接收用户请求，根据所述用户请求调用相应的智能合约，将用户请求信息通过所述连接通道同步至所有网络节点，存储于所述区块链网络的公共账本中。

本申请之计算机非易失性可读存储介质的具体实施方式与上述基于区块链的身份管理方法、装置和电子设备的具体实施方式大致相同，在此不再赘述。

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、装置、物品或者方法不仅包括那些要素，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、装置、物品或者方法所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括该要素的过程、装置、物品或者方法中还存在另外的相同要素。

上述本申请实施例序号仅仅为了描述，不代表实施例的优劣。通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到上述实施例方法可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在如上所述的一个存储介质(如 ROM/RAM、磁碟、光盘)中，包括若干指令用以使得一台终端设备(可以是手机，计算机，服务器，或者网络设备等)执行本申请各个实施例所述的方法。

以上仅为本申请的优选实施例，并非因此限制本申请的专利范围，凡是利用本申请说明书及附图内容所作的等效结构或等效流程变换，或直接或间接运用在其他相关的技术领域，均同理包括在本申请的专利保护范围内。

权 利 要 求 书

1. 一种基于区块链的身份管理方法，应用于电子设备，其特征在于，包括：

根据应用系统的用户模型分别编写智能合约；

构建区块链网络，所述区块链网络包括多个网络节点、多个应用系统和公共账本，每个应用系统均对应至少一个网络节点，各个网络节点通过共识机制自动同步区块链数据；

建立所述区块链网络中各个应用系统之间的连接通道，在所述连接通道上部署智能合约；

通过应用系统接收用户请求，根据所述用户请求调用相应的智能合约，将用户请求信息通过所述连接通道同步至所有网络节点，存储于所述区块链网络的公共账本中。

2. 根据权利要求 1 所述的基于区块链的身份管理方法，其特征在于，将用户请求信息通过所述连接通道同步至所有网络节点的步骤之后，还包括：通过应用系统接收用户的登录请求，应用系统通过调用对应的智能合约，匹配用户的登录信息与所述公共账本中存储的注册信息，若匹配成功，则用户在所述应用系统中有登录权限，若匹配失败，则用户在所述应用系统中没有登录权限。

3. 根据权利要求 2 所述的基于区块链的身份管理方法，其特征在于，通过应用系统接收用户的登录请求的步骤之前，还包括：通过应用系统接收用户的注册请求，应用系统通过调用对应的智能合约，将所述注册请求对应的注册信息写入所述区块链网络，存储于所述公共账本中。

4. 根据权利要求 1 所述的基于区块链的身份管理方法，其特征在于，所述区块链网络还包括多个私有账本，所述私有账本与所述应用系统一一对应，所述公共账本中仅保留每个私有账本的哈希值。

5. 根据权利要求 1 所述的基于区块链的身份管理方法，其特征在于，所述智能合约包括用户注册模块、用户验证模块、登录凭证获取模块、声纹录入模块、指纹录入模块和人脸识别图像录入模块中的一种或多种。

6. 根据权利要求 1 所述的基于区块链的身份管理方法，其特征在于，根

据所述用户请求调用相应的智能合约的步骤包括：响应所述用户请求；通过封装的 java-sdk 调用与所述用户请求对应的智能合约。

7. 根据权利要求 1 所述的基于区块链的身份管理方法，其特征在于，所述身份管理方法还包括：根据用户信息通过编写配置文件配置控制策略，通过所述网络节点根据所述控制策略检测所述用户权限。

8. 根据权利要求 7 所述的基于区块链的身份管理方法，其特征在于，通过应用系统接收用户请求的步骤之后，还包括：对所述用户请求进行验证，匹配所述用户请求与用户权限，若匹配成功，则通过验证，响应所述用户请求，若匹配失败，则未通过验证，拒绝所述用户请求。

9. 根据权利要求 7 所述的基于区块链的身份管理方法，其特征在于，所述控制策略包括自主型访问控制策略、系统强制性访问控制策略、基于角色的访问控制策略和基于属性证书的访问控制策略中的一种。

10. 根据权利要求 1 所述的基于区块链的身份管理方法，其特征在于，所述身份管理方法还包括：通过所述网络节点共享各个应用系统的用户交易信息，所述用户交易信息包括交易类型标识、应用系统标识、用户设备标识、用户身份标识中的一种或多种。

11. 根据权利要求 1 所述的基于区块链的身份管理方法，其特征在于，所述身份管理方法还包括：生成用户操作报表，所述操作报表包括用户的操作时间、操作类型、操作内容。

12. 根据权利要求 11 所述的基于区块链的身份管理方法，其特征在于，生成用户操作报表的步骤包括：

响应用户请求，记录当前用户的操作记录；将所述操作记录生成数据区块；将所述数据区块写入所述区块链网络中；对所述数据区块中的存储数据进行处理，生成当前用户的操作报表。

13.一种基于区块链的身份管理装置，其特征在于，包括：

合约生成模块，用于根据应用系统的用户模型分别编写智能合约；

区块链构建模块，用于构建区块链网络，所述区块链网络包括多个网络节点、多个应用系统和公共账本，每个应用系统均对应至少一个网络节点，各个网络节点通过共识机制自动同步区块链数据；

通道建立模块，用于建立所述区块链网络中各个应用系统之间的连接通

道，在所述连接通道上部署智能合约；

存储模块，用于通过应用系统接收用户请求，根据所述用户请求调用相应的智能合约，将用户请求信息通过所述连接通道同步至所有网络节点，存储于所述区块链网络的公共账本中。

14.根据权利要求 13 所述的基于区块链的身份管理装置，其特征在于，所述区块链网络还包括多个私有账本，所述私有账本与所述应用系统一一对应，所述公共账本中仅保留每个私有账本的哈希值。

15.根据权利要求 13 所述的基于区块链的身份管理装置，其特征在于，所述身份管理装置还包括：权限检测模块，根据用户信息通过编写配置文件配置控制策略，通过所述网络节点根据所述控制策略检测所述用户权限。

16. 根据权利要求 15 所述的基于区块链的身份管理装置，其特征在于，所述身份管理装置还包括验证模块，在通过应用系统接收用户请求之后，对所述用户请求进行验证，匹配所述用户请求与用户权限，若匹配成功，则通过验证，响应所述用户请求，若匹配失败，则未通过验证，拒绝所述用户请求。

17. 根据权利要求 13 所述的基于区块链的身份管理装置，其特征在于，所述身份管理装置还包括报表生成模块，用于生成用户操作报表。

18. 根据权利要求 17 所述的基于区块链的身份管理装置，其特征在于，所述报表生成模块包括：记录单元，响应用户请求，记录当前用户的操作记录；区块生成单元，将所述操作记录生成数据区块；区块写入单元，将所述数据区块写入所述区块链网络中；报表生成单元，对所述数据区块中的存储数据进行处理，生成当前用户的操作报表。

19. 一种电子设备，其特征在于，该电子设备包括：

处理器和存储器，所述存储器中包括基于区块链的身份管理程序，所述基于区块链的身份管理程序被所述处理器执行时实现如权利要求1至12中任一项所述的基于区块链的身份管理方法。

20. 一种计算机非易失性可读存储介质，其特征在于，所述计算机非易失性可读存储介质中包括基于区块链的身份管理程序，所述基于区块链的身份管理程序被处理器执行时，实现如权利要求 1 至 12 中任一项所述的基于区块链的身份管理方法。

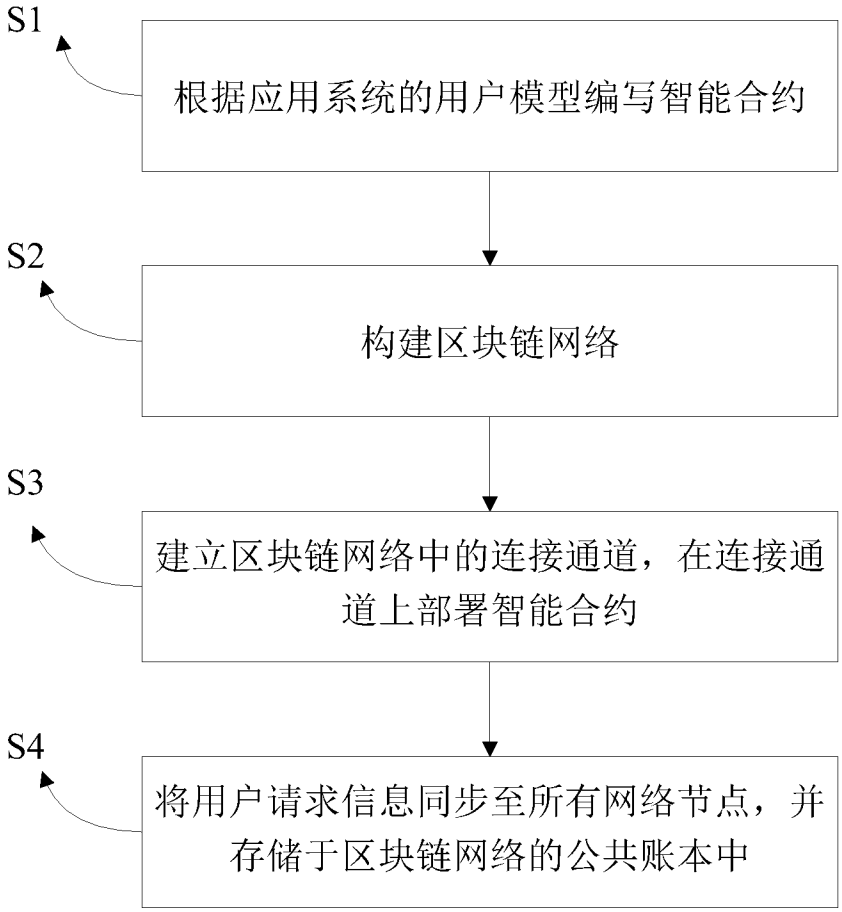
S1
根据应用系统的用户模型编写智能合约
S2
构建区块链网络
S3
建立区块链网络中的连接通道，在连接通道上部署智能合约
S4
将用户请求信息同步至所有网络节点，并存储于区块链网络的公共账本中

图 1

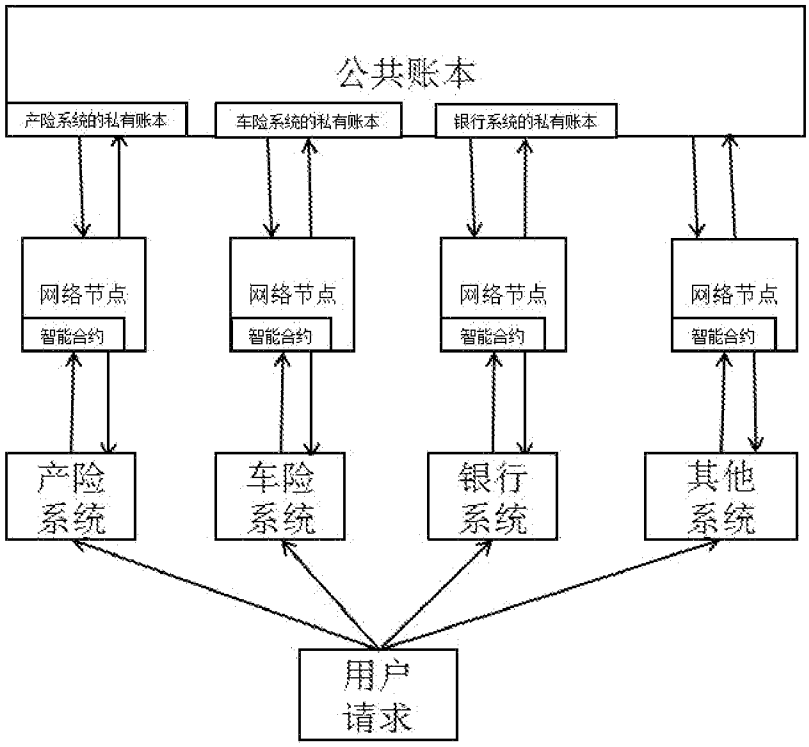
公共账本
产险系统的私有账本
车险系统的私有账本
银行系统的私有账本
网络节点
智能合约
网络节点
智能合约
网络节点
智能合约
网络节点
智能合约
产险系统
车险系统
银行系统
其他系统
用户请求

图 2


身份管理装置
合约生成模块1
区块链构建模块2
通道建立模块3
存储模块4

图 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2019/117804

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/32(2013.01)i; H04L 29/06(2006.01)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)

H04L G06F

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)

CNABS; CNTXT; CNKI; VEN; WOTXT; EPTXT; USTXT; 3GPP: 区块链, 分布式账本, 分布式总账, 多个, 系统, 应用, 通信, 登录, 认证, 身份, 用户, 请求, 智能合约, 单点登录, blockchain, block chain, distributed ledger, multi, system, application, communication, log, register, authentic, identifier, user, request, smart contract

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 109889503 A (PING'AN TECHNOLOGY (SHENZHEN) CO., LTD.) 14 June 2019 (2019-06-14) claims 1-10	1-20
A	CN 107196966 A (BEIJING TRUSTDO TECHNOLOGY CO., LTD.) 22 September 2017 (2017-09-22) entire document	1-20
A	CN 108156159 A (ZHISHU LINK NETWORK TECHNOLOGY CHENGDU CO., LTD.) 12 June 2018 (2018-06-12) entire document	1-20
A	US 2018089641 A1 (THE TORONTO DOMINION BANK) 29 March 2018 (2018-03-29) entire document	1-20

☐ 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
25 January 2020	**13 February 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
Information on patent family members

International application No.
PCT/CN2019/117804

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 109889503 A	14 June 2019	None	
CN 107196966 A	22 September 2017	None	
CN 108156159 A	12 June 2018	None	
US 2018089641 A1	29 March 2018	None	

国际检索报告

国际申请号
PCT/CN2019/117804

A. 主题的分类

G06F 21/32(2013.01)i; H04L 29/06(2006.01)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)

H04L G06F

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）)

CNABS;CNTXT;CNKI;VEN;WOTXT;EPTXT;USTXT;3GPP:区块链，分布式账本，分布式总账，多个，系统，应用，通信，登录，认证，身份，用户，请求，智能合约，单点登录，blockchain，block chain，distributed ledger，multi，system，application，communication，log，register，authentic，identifier，user，request，smart contract

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 109889503 A (平安科技深圳有限公司) 2019年 6月 14日 (2019-06-14) 权利要求1-10	1-20
A	CN 107196966 A (北京信任度科技有限公司) 2017年 9月 22日 (2017-09-22) 全文	1-20
A	CN 108156159 A (质数链网科技成都有限公司) 2018年 6月 12日 (2018-06-12) 全文	1-20
A	US 2018089641 A1 (THE TORONTO DOMINION BANK) 2018年 3月 29日 (2018-03-29) 全文	1-20

☐ 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 1月 25日	2020年 2月 13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 朱秀玲 电话号码 86-(010)-62089127

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2019/117804

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	109889503	A	2019年 6月 14日	无	
CN	107196966	A	2017年 9月 22日	无	
CN	108156159	A	2018年 6月 12日	无	
US	2018089641	A1	2018年 3月 29日	无	