(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
2024 年 10 月 3 日 (03.10.2024)

WIPO | PCT

(10) 国际公布号
WO 2024/197879 A1

(51) 国际专利分类号:
G06F 21/60 (2013.01) *H04L 9/32* (2006.01)

(21) 国际申请号: PCT/CN2023/085649

(22) 国际申请日: 2023 年 3 月 31 日 (31.03.2023)

(25) 申请语言: 中文

(26) 公布语言: 中文

(71) 申请人: 京东方科技集团股份有限公司 **(BOE TECHNOLOGY GROUP CO., LTD.)** [CN/CN]; 中国北京市朝阳区酒仙桥路 10 号, Beijing 100015 (CN)。 北京京东方技术开发有限公司 **(BEIJING BOE TECHNOLOGY DEVELOPMENT CO., LTD.)** [CN/CN]; 中国北京市大兴区北京经济技术开发区地泽路 9 号 1 幢 407 室, Beijing 100176 (CN)。

(72) 发明人: 褚婋 **(CHU, Xiao)**; 中国北京市大兴区北京经济技术开发区地泽路 9 号, Beijing 100176 (CN)。 张宁 **(ZHANG, Ning)**; 中国北京市大兴区北京经济技术开发区地泽路 9 号, Beijing 100176 (CN)。 苗雨 **(MIAO, Yu)**; 中国北京市大兴区北京经济技术开发区地泽路 9 号, Beijing 100176 (CN)。 卞雪达 **(BIAN, Xueda)**; 中国北京市大兴区北京经济技术开发区地泽路 9 号, Beijing 100176 (CN)。 吴新银 **(WU, Xinyin)**; 中国北京市大兴区北京经济技术开发区地泽路 9 号, Beijing 100176 (CN)。 张洪雷 **(ZHANG, Honglei)**; 中国北京市大兴区北京经济技术开发区地泽路 9 号, Beijing 100176 (CN)。

(74) 代理人: 中科专利商标代理有限责任公司 **(CHINA SCIENCE PATENT & TRADEMARK AGENT LTD.)**;

WO 2024/197879 A1

(54) **Title:** BLOCKCHAIN DATA PROCESSING METHOD, PLATFORM, SYSTEM AND APPARATUS, AND ELECTRONIC DEVICE

(54) 发明名称: 区块链数据处理方法、平台、系统、装置和电子设备

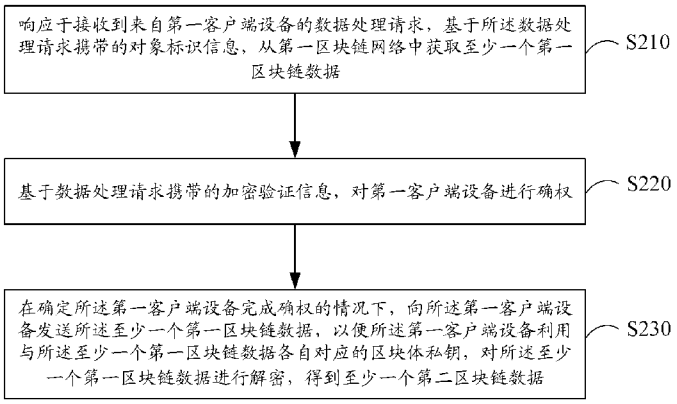

图 2

S210 In response to receiving a data processing request from a first client device, obtain at least one piece of first blockchain data from a first blockchain network on the basis of object identification information carried by the data processing request

S220 Perform right confirmation on the first client device on the basis of encrypted verification information carried by the data processing request

S230 When it is determined that the first client device completes right confirmation, send the at least one piece of first blockchain data to the first client device, so that the first client device decrypts the at least one piece of first blockchain data by using a block private key respectively corresponding to the at least one piece of first blockchain data to obtain at least one piece of second blockchain data

(57) **Abstract:** The present disclosure provides a blockchain data processing method, platform, system and apparatus, an electronic device, and a storage medium. The method comprises: in response to receiving a data processing request from a first client device, obtaining at least one piece of first blockchain data from a first blockchain network on the basis of object identification information carried by the data processing request; performing right confirmation on the first client device on the basis of encrypted verification information carried by the data processing request; and when it is determined that the first client device completes right confirmation,

[见续页]

中国北京市海淀区西三环北路87号4-312室, Beijing 100089 (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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, 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, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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, ME, 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))。

sending the at least one piece of first blockchain data to the first client device, so that the first client device decrypts the at least one piece of first blockchain data by using a block private key respectively corresponding to the at least one piece of first blockchain data to obtain at least one piece of second blockchain data.

(57) 摘要: 本公开提供了一种区块链数据处理方法、平台、系统、装置、电子设备和存储介质。该方法包括：响应于接收到来自第一客户端设备的数据处理请求，基于数据处理请求携带的对象标识信息，从第一区块链网络中获取至少一个第一区块链数据；基于数据处理请求携带的加密验证信息，对第一客户端设备进行确权；以及在确定第一客户端设备完成确权的情况下，向第一客户端设备发送至少一个第一区块链数据，以便第一客户端设备利用与至少一个第一区块链数据各自对应的区块体私钥，对至少一个第一区块链数据进行解密，得到至少一个第二区块链数据。

区块链数据处理方法、平台、系统、装置和电子设备

技术领域

本公开涉及区块链技术领域，更具体地，涉及一种区块链数据处理方法、平台、系统、装置、电子设备和存储介质。

背景技术

区块链是一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构，并以密码学方式保证的不可篡改和不可伪造的分布式账本。区块链网络的链上数据是一个数据孤岛，不同的区块链之间无法做到互联互通，这阻碍了不同区块链间数据应用生态的进一步发展。为了提供区块链数据的利用效率，可以利用跨链数据处理方法来实现区块链间的数据共享。

发明内容

本公开提供了一种区块链数据处理方法、平台、系统、装置、电子设备和存储介质。

根据本公开的一方面，提供了一种区块链数据处理方法，包括：响应于接收到来自第一客户端设备的数据处理请求，基于上述数据处理请求携带的对象标识信息，从第一区块链网络中获取至少一个第一区块链数据；基于上述数据处理请求携带的加密验证信息，对上述第一客户端设备进行确权；以及在确定上述第一客户端设备完成确权的情况下，向上述第一客户端设备发送上述至少一个第一区块链数据，以便上述第一客户端设备利用与上述至少一个第一区块链数据各自对应的区块体私钥，对上述至少一个第一区块链数据进行解密，得到至少一个第二区块链数据。

根据本公开的另一方面，提供了一种区块链数据处理平台，包括：区块链数据源管理模块，被配置为响应于接收到来自第一客户端设备的数据处理请求，基于上述数据处理请求携带的对象标识信息，从第一区块链网络中获取至少一个第一区块链数据；私钥控制模块，被配置为基于上述数据处理请求携带的加密验证信息，对上述第一客户端设备进行确权；以及数据处理模块，被配置为在确定上述第一客户端设备完成确权的情况下，向上述第一客户端设备发送上述至少一个第一区块链数据，以便上述第一客户端设备利用与上述至少一个第一区块链数据各自对应的区块体私钥，对上述至少一个第一区块链数据进行解密，得到至少一个第二区块链数据。

根据本公开的另一方面，提供了一种区块链数据处理系统，包括：第一客户端设备、第一区块链网络、区块链数据处理平台和分布式私钥网络；其中，上述区块链数据处理平台被配置为：响应于接收到来自第一客户端设备的数据处理请求，基于上述数据处理请求携带的对象标识信息，从第一区块链网络中获取至少一个第一区块链数据；基于上述数据处理请求携带的加密验证信息，对上述第一客户端设备进行确权；在确定上述第一客户端设备完成确权的情况下，向上述第一客户端设备发送上述至少一个第一区块链数据；上述第一客户端设备被配置为：利用与上述至少一个第一区块链数据各自对应的区块体私钥，对上述至少一个第一区块链数据进行解密，得到至少一个第二区块链数据。

根据本公开的另一方面，提供了一种区块链数据处理装置，包括：第一获取模块，用于响应于接收到来自第一客户端设备的数据处理请求，基于上述数据处理请求携带的对象标识信息，从第一区块链网络中获取至少一个第一区块链数据；确权模块，用于基于上述数据处理请求携带的加密验证信息，对上述第一客户端设备进行确权；以及第一发送模块，用于在确定上述第一客户端设备完成确权的情况下，向上述第一客户端设备发送上述至少一个第一区块链数据，以便上述第一客户端设备利用与上述至少一个第一区块链数据各自对应的区块体私钥，对上述至少一个第一区块链数据进行解密，得到至少一个第二区块链数据。

根据本公开的另一方面，提供了一种电子设备，包括存储器和处理器，存储器中存储有处理器可执行的指令，指令在由处理器执行时使处理器执行实现如上所述的方法。

根据本公开的另一方面，提供了一种存储有计算机指令的非瞬时计算机可读存储介质，其中，计算机指令用于使计算机执行实现如上所述的方法。

根据本公开的另一方面，提供了一种计算机程序产品，包括计算机程序，计算机程序在被处理器执行时实现如上所述的方法。

应当理解，本部分所描述的内容并非旨在标识本公开的实施例的关键或重要特征，也不用于限制本公开的范围。本公开的其它特征将通过以下的说明书而变得容易理解。

附图说明

附图用于更好地理解本方案，不构成对本公开的限定。其中：

图1示意性示出了根据本公开实施例的可以应用区块链数据处理方法的示例性系统架构。

图2示意性示出了根据本公开实施例的区块链数据处理方法的流程图。

图 3 示意性示出了根据本公开另一实施例的区块链数据处理方法的流程图。

图 4 示意性示出了根据本公开又一实施例的区块链数据处理方法的流程图。

图 5A 示意性示出了根据本公开实施例的区块链数据异步查看方法的示意图。

图 5B 示意性示出了根据本公开实施例的区块链数据同步查看方法的示意图。

图 6 示意性示出了根据本公开实施例的区块链数据共享方法的示意图。

图 7 示意性示出了根据本公开实施例的区块链数据调用方法的示意图。

图 8 示意性示出了根据本公开实施例的区块链数据处理平台的示意图。

图 9 示意性示出了根据本公开实施例的区块链数据处理系统的示意图。

图 10 示意性示出了根据本公开实施例的区块链数据处理装置的框图。

图 11 示意性示出了根据本公开实施例的适于实现区块链数据处理方法的电子设备的框图。

具体实施方式

以下，将参照附图来描述本公开的实施例。但是应该理解，这些描述只是示例性的，而并非要限制本公开的范围。在下面的详细描述中，为便于解释，阐述了许多具体的细节以提供对本公开实施例的全面理解。然而，明显地，一个或多个实施例在没有这些具体细节的情况下也可以被实施。此外，在以下说明中，省略了对公知结构和技术的描述，以避免不必要地混淆本公开的概念。

在此使用的术语仅仅是为了描述具体实施例，而并非意在限制本公开。在此使用的术语“包括”、“包含”等表明了所述特征、步骤、操作和/或部件的存在，但是并不排除存在或添加一个或多个其他特征、步骤、操作或部件。

在此使用的所有术语（包括技术和科学术语）具有本领域技术人员通常所理解的含义，除非另外定义。应注意，这里使用的术语应解释为具有与本说明书的上下文相一致的含义，而不应以理想化或过于刻板的方式来解释。

在使用类似于“A、B 和 C 等中至少一个”这样的表述的情况下，一般来说应该按照本领域技术人员通常理解该表述的含义来予以解释（例如，“具有 A、B 和 C 中至少一个的系统”应包括但不限于单独具有 A、单独具有 B、单独具有 C、具有 A 和 B、具有 A 和 C、具有 B 和 C、和/或具有 A、B、C 的系统等）。在使用类似于“A、B 或 C 等中至少一个”这样的表述的情况下，一般来说应该按照本领域技术人员通常理解该表述的含义来予以解释（例如，“具有 A、B 或 C 中至少一个的系统”应包括但不限于单独具有 A、

单独具有B、单独具有C、具有A和B、具有A和C、具有B和C、和/或具有A、B、C的系统等）。

在本公开的技术方案中，所涉及的数据（如包括但不限于用户个人信息）的收集、存储、使用、加工、传输、提供、公开和应用等处理，均符合相关法律法规的规定，采取了必要保密措施，且不违背公序良俗。

在本公开的技术方案中，在获取或采集用户个人信息之前，均获取了用户的授权或同意。

需要说明的是，本公开实施例中的流程图所示的操作除非明确说明不同操作之间存在执行的先后顺序，或者不同操作在技术实现上存在执行的先后顺序，否则，多个操作之间的执行顺序可以不分先后，多个操作也可以同时执行。

为了适应信息化发展和业务扩张的需求，企业一般会建设业务信息化系统，如ERP（Enterprise Resource Planning，企业资源计划）、OA（Office Automation，办公自动化）、CRM（Customer Relationship Management，客户关系管理）等。业务信息化系统可以规范业务流程，形成标准化的业务模式，并通过系统数据库沉淀业务数据，为企业积累数据资产。同时，也伴随着数据隐私问题逐渐受大众关注，区块链因其去中心化、不可篡改、加密存储等特性，开始逐步取代系统数据库作为业务信息化系统的存储单元。然而，区块链网络的链上数据是一个数据孤岛，不同的区块链之间无法做到互联互通，无法统一进行利用，这阻碍了不同区块链间数据应用生态的进一步发展。

以医疗区块链为例，医疗数据的建设中存在许多问题，例如：各机构无法快速便捷地共享数据；医院的系统和软件大多是通过第三方软件公司开发并维护的，但市场上这些第三方公司鱼龙混杂、存在安全漏洞，而医疗数据又具有高度隐私性、高价值性；医疗数据的归属问题和访问权限同时存在争议等。在相关技术中，一般选择将医疗数据直接存储在区块链上，然后，这样会大大增加区块链网络的开支，使得吞吐量成为阻碍技术发展的瓶颈。同时，也存在着数据归属权混乱的问题，即使是患者本人也不能拥有全部的医疗数据，医疗数据保存在医院又会造成数据共享手续繁杂，大规模的数据共享变得不现实。

有鉴于此，本公开实施例提供了一种区块链数据处理方法。响应于接收到来自第一客户端设备的数据处理请求，基于数据处理请求携带的对象标识信息，从第一区块链网络中获取至少一个第一区块链数据；基于数据处理请求携带的加密验证信息，对第一客户端设备进行确权；以及在确定第一客户端设备完成确权的情况下，向第一客户端设备

发送至少一个第一区块链数据，以便第一客户端设备利用与至少一个第一区块链数据各自对应的区块体私钥，对至少一个第一区块链数据进行解密，得到至少一个第二区块链数据。

为了便于理解，下面首先对本公开实施例所涉及的相关概念进行说明。

区块链是一种利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的安全和利用由自动化脚本代码组成的智能合约集体维护可靠数据库的解决方案，因此，区块链具有开放、去中心化、信息共享、防篡改和可追溯等基本特性。区块链可以用区块来取代对中心服务器的依赖。

区块可以是一个被包括在区块链中聚合了数据的容器数据结构。区块可以包括区块头和区块体。区块头可以包括版本、时间戳、父区块哈希值、随机数、难度系数和默克尔根。时间戳可以表征区块创建时刻。父区块哈希值可以用于引用上一个区块。区块体可以包括交易详情、交易计数器和区块大小。

智能合约是存储在区块链中的可执行代码。可执行代码中确定了智能合约的执行条件以及业务处理逻辑，即，确定了启动智能合约的条件以及在该智能合约启动后如何处理接收到的业务处理请求。智能合约在存储于区块链之后，就难以被编辑或者修改。例如，智能合约的执行操作可以根据事件进行触发。例如，智能合约的执行会在区块链上被记录为一个交易，并记录在区块链中。

根据网络范围，可以将区块链划分为公有链、私有链、联盟链和混合链。联盟链是指由若干机构共同参与和管理的区块链，每个机构都可以运行至少一个区块链节点。联盟链的数据只允许联盟链系统中的机构进行读写和交易，并通过数字证书的方式实现基于 PKI（Public Key Infrastructure，公钥基础设施）的身份管理体系、交易或提案的发起，以参与方共同签名验证来达成共识。在本公开实施例中，可以根据实际业务需求确定区块链的类型，在此不作限定。例如，区块链网络是联盟链。

区块链网络可以包括多个区块链节点。区块链节点是通过 P2P（Peer to Peer，对等网络）实现通信。区块链节点既可以是客户端，也可以是服务端，即，区块链节点既可以向其他区块链节点请求服务， 也可以为其他区块链节点或是外部应用提供服务。

图 1 示意性示出了根据本公开实施例的可以应用区块链数据处理方法的示例性系统架构。需要注意的是，图 1 所示仅为可以应用本公开实施例的系统架构的示例，以帮助本领域技术人员理解本公开的技术内容，但并不意味着本公开实施例不可以用于其他设备、系统、环境或场景。

如图 1 所示，根据该实施例的系统架构 100 可以包括终端设备 101、服务器 102 和区块链网络 103。

终端设备 101 可以是具有显示屏的各种电子设备，包括但不限于智能手机、平板电脑、膝上型便携计算机和台式计算机等。

服务器 102 可以是提供各种服务的各种类型的服务器。例如，服务器可以是云服务器，又称为云计算服务器或云主机，是云计算服务体系中的一项主机产品，以解决了传统物理主机与 VPS 服务（Virtual Private Server，VPS）中，存在的管理难度大，业务扩展性弱的缺陷。服务器也可以为边缘服务器。服务器也可以为分布式系统的服务器，或者是结合了区块链的服务器。

区块链网络 103 可以包括多个区块链节点，每个区块链节点可以是客户端设备或服务器。

服务器 102 与终端设备 101 之间、服务器 102 与区块链网络 103 的各个区块链节点之间可以通过网络进行通信，网络可以包括各种连接类型，例如有线和/或无线通信链路等。

需要说明的是，本公开实施例所提供的区块链数据处理方法一般可以由服务器 102 执行。相应地，本公开实施例所提供的区块链数据处理装置也可以设置于服务器 102 中。

例如，用户可以在终端设备 101 的客户端应用中进行输入、选择等操作，终端设备 101 可以基于该输入、选择等操作，生成数据处理请求，并将数据处理请求发送给服务器 102。服务器 102 可以响应于接收到来自终端设备 101 的数据处理请求，基于数据处理请求携带的对象标识信息，从区块链网络 103 中获取第一区块链数据。同时，服务器 102 可以基于数据处理请求携带的加密验证信息，对终端设备 101 进行确权。在确定终端设备 101 完成确权的情况下，向终端设备 101 返回第一区块链数据。终端设备 101 可以利用与第一区块链数据对应的区块体私钥对第一区块链数据进行解密，得到第二区块链数据。

应该理解，图 1 中的终端设备、服务器和区块链网络的数目仅仅是示意性的。根据实现需要，可以具有任意数目的终端设备、服务器和区块链网络。

图 2 示意性示出了根据本公开实施例的区块链数据处理方法的流程图。

如图 2 所示，该方法包括操作 S210~S230。

在操作 S210，响应于接收到来自第一客户端设备的数据处理请求，基于所述数据处理请求携带的对象标识信息，从第一区块链网络中获取至少一个第一区块链数据。

在操作 S220，基于数据处理请求携带的加密验证信息，对第一客户端设备进行确权。

在操作 S230，在确定所述第一客户端设备完成确权的情况下，向所述第一客户端设备发送所述至少一个第一区块链数据，以便所述第一客户端设备利用与所述至少一个第一区块链数据各自对应的区块体私钥，对所述至少一个第一区块链数据进行解密，得到至少一个第二区块链数据。

根据本公开的实施例，客户端设备可以是安装有各种客户端应用的电子设备。根据不同划分角度，可以将客户端应用分为不同类型的客户端应用。例如，根据客户端应用提供的服务功能，可以将客户端应用分为个人客户端应用和服务客户端应用。个人客户端应用可以指用户利用客户端应用提供的功能进行业务操作的客户端应用。服务客户端应用可以指支持用户进行业务服务的客户端应用。根据客户端应用的开发框架，可以将客户端应用分为程序客户端应用和网页客户端应用。程序客户端应用可以指加载应用程序（Application，APP）的客户端应用。网页客户端应用可以指 Web 客户端应用。Web 客户端应用可以包括 Web 浏览器。根据用户是否进行了注册操作，可以将客户端应用划分为注册客户端应用和非注册客户端应用。注册客户端应用可以指用户在使用客户端应用自身提供的功能和加载于客户端应用的应用提供的功能中的至少一项的过程中进行了注册操作的客户端应用。非注册客户端应用可以指用户在使用客户端应用自身提供的功能和加载于客户端应用的应用提供的功能中的过程中未进行注册操作的客户端应用。程序客户端应用可以是个人客户端应用、服务客户端应用、注册客户端应用或非注册客户端应用。网页客户端应用可以是个人客户端应用、服务客户端应用、注册客户端应用或非注册客户端应用。

根据本公开的实施例，数据处理请求可以是由第一客户端设备发起，或者由其他客户端设备发起并由第一客户端设备进行转发的，用于从各个区块链网络中获取区块链数据的请求。数据处理请求可以是由客户端设备根据用户的输入、选择等操作而生成的。输入操作例如可以是用户在客户端设备中客户端应用的界面的输入控件中，通过键盘、麦克风等输入设备进行的信息输入操作。选择操作例如可以是用户在客户端设备中客户端应用的界面的选择控件中，采用鼠标选择、触控选择等方式进行的信息选择操作。第一客户端设备可以将数据处理请求发送给区块链数据处理平台。

根据本公开的实施例，对象标识信息可以指用于唯一表示数据处理请求的请求方身份的信息。数据处理请求的请求方可以指控制客户端设备来发起该数据处理请求的用户，

相应的，对象标识信息可以指该用户的用户名、用户ID、用户身份证号码等信息。

根据本公开的实施例，第一区块链网络可以是由区块链数据处理平台创建的区块链网络，区块链数据处理平台的服务端设备可以至少作为第一区块链网络的一个记账节点。第一区块链网络的类型可以包括但不限于公有链、联盟链、私有链、侧链、支链等。优选地，由于公有链网络的TPS（transactionspersecond，每秒交易数）明显低于联盟链网络或私有链网络，例如，以太坊区块链的TPS一般为20，而私有链的TPS可以接近10万，为了提高区块链数据的读写效率，第一区块链网络的类型可以为联盟链网络或私有链网络，相应的，区块链数据处理平台的服务端设备可以作为联盟链网络或私有链网络中的被授权节点。

根据本公开的实施例，第一区块链网络中记录的区块链数据可以是来源于不同数据源的用户数据，在获取用户的授权后，可以将用户数据打包成区块，并将区块在第一区块链网络中上链。

根据本公开的实施例，基于对象标识信息来获取第一区块链数据，可以是通过将对象标识信息与第一区块链网络中每个区块的区块头的相关方标识进行匹配的方式，来确定相关的目标区块，该相关的目标区块的区块体数据即需要获取的第一区块链数据。

根据本公开的实施例，第一区块链数据中可以包括第一区块链网络的一个或多个区块的区块体数据。

根据本公开的实施例，加密验证信息可以包括用于对第一客户端设备进行身份认证及权限认证的信息。例如，加密验证信息可以包括用户名和密码、生物特征信息、预设的特定问题的答案、密码锁组合等。作为一种可选实施方式，加密验证信息可以是对上述种类的信息进行加密处理后得到的，例如，可以对上述种类的信息进行哈希计算，得到的哈希值即该加密验证信息。进一步地，为了保障加密验证信息在信息传输过程中的安全性，还可以借助数字签名方法、加密方法等对得到的哈希值进行加密，从而得到机密验证信息。在基于加密验证信息确定第一客户端设备通过身份认证后，还可以利用权限管理方法，例如，DAC（Discretionary Access Control，主动访问控制）、MAC（Mandatory Access Control，强制访问控制）、RBAC（Role-based Access Control，基于角色的访问控制）等来确定第一客户端设备的权限，权限可以包括数据访问权、数据所有权等。例如，在确定第一客户端设备具有数据访问权的区块下，可以从第一区块链网络中获取第一区块链数据，或者，可以获取对第一区块链数据进行解密所得到的第二区块链数据。在确定第一客户端设备具有数据所有权的区块下，还可以在接收到来自第一客户端设备的共

享、修改等请求的区块下，对第一区块链网络中的第一区块链数据作共享、修改等处理。

根据本公开的实施例，第二区块链数据可以是对应于第一区块链数据的明文数据。

根据本公开的实施例，可以基于加密验证信息进行第一客户端设备的确权，并在确定完成确权的情况下，可以确定第一客户端设备具有获取第一区块链数据的权限，此时可以将第一区块链数据返回至第一客户端设备。通过上述技术手段，设备间的数据通信链路均只进行密文数据的传输，且用于第一区块链数据解密的区块链私钥不会以明文或密文的方式向外暴露，因此可以有效地保障区块链网络数据的安全性，有助于数据的进一步保真、防篡改。

根据本公开的实施例，分布式私钥网络可以是由多个节点构成的分布式网络。用户在区块链网络中进行注册时所生成的区块体私钥可以分布式地存储在该分布式私钥网络的特定节点上。区块体私钥在分布式私钥网络中的存储形式不作限定，例如，可以是将区块体私钥切分为多份子密钥，每一份子密钥可以存储在一个节点中。或者，也可以将区块体私钥进行再次加密，将再次加密后的区块体私钥存储在一个节点中，并将再次加密所使用的密钥存储在其他节点中。

根据本公开的实施例，基于加密验证信息对第一客户端设备进行确权可以包括区块链数据处理平台和分布式私钥网络依次对第一客户端设备进行确权。具体地，加密验证信息可以是由第一客户端设备利用对象私钥对私钥摘要信息进行数字签名而得到的，私钥摘要信息可以是由第一客户端设备对与至少一个第一区块链数据各自对应的区块体私钥进行拼接和哈希计算而得到的。基于数据处理请求携带的加密验证信息，对第一客户端设备进行确权可以包括如下操作：

基于对象标识信息，得到对象公钥，其中，对象公钥与对象私钥相对应。利用对象公钥对加密验证信息进行验签，得到第一摘要信息，其中，在加密验证信息验签成功的情况下，第一摘要信息为私钥摘要信息。向分布式私钥网络发送对象标识信息和第一摘要信息，以便分布式私钥网络根据对象标识信息，确定至少一个区块链体私钥，对至少一个区块体私钥进行拼接和哈希计算，得到第二摘要信息，并基于第一摘要信息和第二摘要信息的匹配结果，确定第一客户端设备的确权结果。

根据本公开的实施例，对象标识信息中可以包括能够表示第一客户端设备和/或数据处理请求的请求方的信息，通过该信息，区块链数据处理平台可以从存储单元中获取与第一客户端设备和/或数据处理请求的请求方对应的对象公钥。

根据本公开的实施例，利用对象公钥对加密验证信息进行验签可以是利用对象公钥

对加密验证信息进行解密。

根据本公开的实施例，第一摘要信息可以与私钥摘要信息相同，也可以与私钥摘要信息不同。具体地，当在第一客户端设备到区块链数据处理平台的数据传输过程中，对象标识信息和加密验证信息中的任意一个被篡改或发生扰动的情况下，得到的第一摘要信息可以与私钥摘要信息存在区别。当对象标识信息和加密验证信息均无误时，得到的第一摘要信息可以为私钥摘要信息。进一步地，当第一摘要信息与私钥摘要信息不同的情况下，第一摘要信息必然与第二摘要信息不匹配。

根据本公开的实施例，私钥摘要信息、第一摘要信息和第二摘要信息可以均表示为一个哈希值，上述哈希值可以采用相同的哈希算法计算得到，哈希算法可以根据具体应用场景进行选择，在此不作限定。

根据本公开的实施例，可以在确定第一摘要信息和第二摘要信息相匹配的情况下，得到表示第一客户端设备完成确权的确权结果，并在确定第一摘要信息和第二摘要信息不匹配的情况下，得到表示第一客户端设备未完成确权的确权结果。

根据本公开的实施例，通过区块链数据处理平台和分布式私钥网络依次对第一客户端设备进行确权的方式，可以避免数据中心化，从而保障数据安全。

根据本公开的实施例，在请求方首次发起数据处理请求，即在第一区块链网络中不存在至少一个第一区块链数据的情况下，可以通过跨链数据获取的方式，从至少一个第二区块链网络中获取至少一个第一区块链数据。

根据本公开的实施例，第二区块链网络可以是业务信息化系统的存储单元。用户可以在第二区块链网络上进行注册和授权，在用户使用该业务信息化系统开展业务的过程中，所产生的业务数据可以被该系统收集，并在对业务数据进行加密后，将加密后的数据在第二区块链网络上链。业务数据可以使用区块体公钥进行加密。区块体公钥可以是用户在第二区块链网络上注册的过程中生成的。例如，用户可以利用客户端设备中配置的加密客户端应用，基于用户输入的字符串来生成区块体公钥和区块体私钥，并将该区块体公钥在注册过程中发送给业务信息化系统。在数据上链时，可以将每个固定时间段内产生的业务数据打包成一个区块，并将该区块在第二区块链网络中上链。该区块的区块头可以包括能够明文查看的上链时间、相关方标识、父区块哈希值等信息。

图 3 示意性示出了根据本公开另一实施例的区块链数据处理方法的流程图。

如图 3 所示，该方法包括操作 S310~S330。

在操作 S310，响应于数据处理请求，在未能从第一区块链网络中获取至少一个第

一区块链数据的情况下，基于对象标识信息，分别对至少一个第二区块链网络进行跨链数据获取，得到至少一个第一区块链数据。

在操作 S320，基于数据处理请求携带的加密验证信息，对第一客户端设备进行确权。

在操作 S330，在确定所述第一客户端设备完成确权的情况下，向所述第一客户端设备发送所述至少一个第一区块链数据，以便所述第一客户端设备利用与所述至少一个第一区块链数据各自对应的区块体私钥，对所述至少一个第一区块链数据进行解密，得到至少一个第二区块链数据。

根据本公开的实施例，未能从第一区块链网络中获取至少一个第一区块链数据，即对象标识信息无法与第一区块链网络包括的多个区块的区块头的任意一个完成匹配。

根据本公开的实施例，操作 S320~S330 的方法可以使用前述实施例中提供的相同或相似的方法来实现，在此不再赘述。

根据本公开的实施例，基于数据处理请求携带的对象标识信息，分别从至少一个区块链网络的每个区块链网络中跨链获取第一区块链数据可以利用跨链方法来实现，该跨链方法例如可以是基于跨链节点的跨链方法，具体地，该跨链方法可以包括如下操作：

对于每个第二区块链网络，确定第二区块链网络的跨链节点。基于跨链节点的节点类型，通过跨链节点来获取第一区块链数据。

根据本公开的实施例，跨链节点可以是能够对外提供通信接口的区块链节点，外部设备可以通过该通信接口，利用约定的通信协议来建立与该跨链节点的通信链路。

根据本公开的实施例，跨链节点的类型可以与第二区块链网络的类型相关，具体地，可以与不同类型的第二区块链网络的节点权限分配相关。例如，在第二区块链网络为联盟链网络的情况下，由于在联盟链网络中，联盟链网络的读取权限、交易权限和记账权限均分配给了被授权节点，外部未授权的节点无法访问。因此，跨链节点可以是联盟链网络中的被授权节点。再例如，在第二区块链网络为私有链网络的情况下，由于在私有链网络中，读取权限是完全私有的，而交易权限和记账权限被分配给了有限的被授权节点。因此，在进行数据读取操作时，跨链节点可以是私有链网络中的被授权节点或未授权节点，而在进行数据更新操作时，跨链节点仅可以是私有链网络中有限的被授权节点。

根据本公开的实施例，再例如，在第二区块链网络为公有链网络的区块下，由于任何人均可以拥有公有链网络的读取权限、交易权限和记账权限。因此，跨链节点可以是公有链网络中的任意节点，如轻节点、全节点等，也可以是公有链网络外的任意节点。

第二区块链网络中的轻节点可以是不储存或维护完整的区块链账本，只储存最小量的状态来作为发送或传递交易信息的节点。轻节点可以仅保存区块链账本中所有区块的区块头，借助区块头中的默克尔根，便能够验证一笔支付交易是否存在。全节点可以是拥有完整区块链账本的节点，全节点需要占用内存同步所有的区块链数据，能够独立校验区块链上的所有交易并实时更新数据，主要负责区块链的交易的广播和验证。不同全节点上记录的数据可以通过共识机制进行同步。

根据本公开的实施例，根据至少一个第二区块链网络中不同第二区块链网络的跨链节点的类型的不同，第一区块链数据的跨链获取方式可以存在区别。

例如，在确定跨链节点为全节点的情况下，可以向跨链节点发送包括对象标识信息的数据获取请求，以便基于跨链节点返回的第一反馈数据，得到第一区块链数据。此时第一区块链数据的获取效率较高。

根据本公开的实施例，第一反馈数据可以是由跨链节点基于对象标识信息，从跨链节点的账本中得到的，第一反馈数据的具体获取方式在此不作限定。跨链节点的账本可以指维持在该跨链节点的存储单元中的完整区块链账本。

根据本公开的实施例，跨链节点返回的第一反馈数据可以是包括一个或多个区块的数据报文。基于第一反馈数据来得到第一区块链数据，可以是将该数据报文包括的一个或多个区块的区块头去除后，并组合或拼接得到第一区块链数据。

根据本公开的实施例，通过将跨链节点直接设置为公有链网络的全节点的方式，可以减少数据获取业务的耗时，节省带宽。

再例如，在确定跨链节点为轻节点的情况下，可以通过跨链节点向第二区块链网络的全节点发送包括对象标识信息的数据获取请求，以便基于全节点通过跨链节点返回的第二反馈数据，得到第一区块链数据。

根据本公开的实施例，第二反馈数据是由全节点基于由跨链节点转发的对象标识信息，从全节点的账本中得到的，第二反馈数据的具体获取方式在此不作限定。全节点的账本可以指维持在该全节点的存储单元中的完整区块链账本。

根据本公开的实施例，轻节点可以作为一个代理节点，将通过接口接收的指令转发给全节点。作为一种可选实施方式，轻节点在进行指令的转发前，还可以利用该轻节点的账本中，各个区块的区块头来对指令进行预验证，对于未通过预验证的指令可以不予转发。例如，在进行支付交易的查询时，可以利用区块头包括的默克尔根进行预验证，即判断该支付交易是否已经被验证过。在确定该支付交易已被验证时，则可以确定该支

付交易已被记录在该第二区块链网络中。

根据本公开的实施例，第二区块链网络中的每个全节点可以表示为一个分布式网络。即全节点在逻辑上可以表示为第二区块链网络中的单个节点，在物理上，该全节点可以由多个分布式节点构成。相应的，全节点的区块链账本可以切分为多个子帐本，多个子帐本可以分布式地存储在多个分布式节点中，从而实现全节点的性能扩展，同时也可以避免数据劫持问题。轻节点可以向全节点中的每个分布式节点广播数据获取请求，多个分布式节点可以分别从各自的子帐本中提取子数据，并将子数据发送给轻节点，轻节点可以将各个子数据进行组合及拼接，以得到第二反馈数据。

根据本公开的实施例，在跨链节点是公有链网络外的任意节点时，该跨链节点可以通过url（UniversalResourceLocator，统一资源定位符）地址、特定接口等来访问公有链网络，并从公有链网络的各个节点中获取第一区块链数据。具体地，对于每个第二区块链网络，在第二区块链网络为公有链网络的情况下，可以向第二区块链网络包括的多个区块链节点广播包括对象标识信息的数据获取请求。并基于多个区块链节点各自的第三反馈数据，得到第一区块链数据。

根据本公开的实施例，第三反馈数据可以是由区块链节点基于对象标识信息，从区块链节点的账本中得到的。

根据本公开的实施例，基于多个区块链节点各自返回的第三反馈数据，得到第一区块链数据可以是对多个第三反馈数据进行比较，以将出现频次最高的第三反馈数据作为第一区块链数据。

根据本公开的实施例，通过借助公有链网络的广播机制，可以进一步扩大数据来源节点的范围，从而提高获取得到的数据的可靠性。

根据本公开的实施例，作为一种可选实施方式，对第一客户端设备进行确权也可以是区块链数据处理平台单独对第一客户端设备进行确权。具体地，在对第一区块链数据进行处理前，可以对第一客户端设备进行确权，以确定请求方是否具有相应的权限。若完成确权，则可以确定请求方具有相应权限，且可以认为获得了该用户的授权，可以继续进行第一区块链数据的解密。若未完成确权，则可以认为该用户可能为非法用户，且未取得合法用户的授权。由于第一区块链数据为密文数据，因此，此时取得的第一区块链数据可以表现为乱码数据，不影响区块链数据的隐私安全。作为一种可选实施方式，也可以先对第一客户端设备进行确权处理，在确认第一客户端设备完成确权的情况下，再基于对象标识信息来从至少一个第二区块链网络中跨链获取第一区块链数据，在此不

作限定。

根据本公开的实施例，确权处理所基于的信息可以是加密验证信息，为了保障加密验证信息是可信的，即该加密验证信息在信息传输过程中未被篡改，可以对原本的验证信息进行加密处理。加密处理的方式可以包括对称加密、非对称加密、数字签名等。以数字签名为例，可以由第一客户端设备使用其所持有的对象私钥对验证信息明文进行加密，以得到加密验证信息。即，加密验证信息可以是由第一客户端设备利用对象私钥对验证信息明文进行数字签名而得到的。

根据本公开的实施例，验证信息明文可以是由第一客户端设备对加密组合信息进行哈希计算得到的。

根据本公开的实施例，对象密钥对可以由第一客户端设备基于随机数、设备编号、设备生成日期等数据而生成的。对象密钥对可以包括对象私钥和对象公钥。对象私钥可以通过烧制刻录在该设备的硬件设施中，从而使得该对象私钥仅由第一客户端设备持有，而无法被外部设备获取。对象公钥可以预先对外公布，以便其他设备利用对象公钥进行验签。

根据本公开的实施例，基于数据处理请求携带的加密验证信息，对第一客户端设备进行确权可以包括如下操作：

基于对象标识信息，得到预留加密组合信息和对象公钥，其中，对象公钥与对象私钥相对应。利用对象公钥对加密验证信息进行验签，得到第一验证信息。对预留加密组合信息进行哈希计算，得到第二验证信息。基于第一验证信息和第二验证信息的匹配结果，确定第一客户端设备的确权结果。

根据本公开的实施例，对象标识信息中可以包括能够表示第一客户端设备的信息，通过该信息，可以从存储单元中获取与第一客户端设备对应的预留加密组合信息和对象公钥。

根据本公开的实施例，加密组合信息可以是数据处理请求的请求方在注册时所填写的信息。例如，加密组合信息可以包括以下至少一项：预设问题的答案文本，密码字符串和生物特征信息。在请求方进行注册时，可以通过设置密保、设置密码找回安全问题等方式，要求请求方设置一个或多个预设问题的答案，预设问题的答案文本即包括请求方在注册时所选择的问题编号，以及所填入的答案。密码字符串可以是请求方在注册时设置的二级密码、安全密码等，也可以是请求方在注册时所输入的随机数或随机字符串。生物特征信息可以包括请求方的人像特征、虹膜、指纹、声纹等信息。生物特征信息可

以由第一客户端设备采集得到。相应的，预留加密组合信息可以是数据处理请求的请求方在注册并填写信息时，由区块链数据处理平台所保存的信息。预留加密组合信息也可以包括以下至少一项：预设问题的答案文本，密码字符串和生物特征信息。

根据本公开的实施例，验证信息明文可以是一个哈希值。该哈希值可以由请求方在发起数据处理请求时直接输入到第一客户端设备。或者，第一客户端设备中可以维持有一张映射表，该映射表的每一项包括了从一个简单信息到哈希值的映射，请求方在发起数据处理请求时，可以输入该简单信息，第一客户端设备可以利用基于该简单信息，从映射表中获取相应的验证信息明文。简单信息可以包括字符串、数字组合等。

根据本公开的实施例，利用对象公钥对加密验证信息进行验签可以是利用对象公钥对加密验证信息进行解密。

根据本公开的实施例，第一验证信息可以与验证信息明文相同，也可以与验证信息明文不同。具体地，当在第一客户端设备到区块链数据处理平台的数据传输过程中，对象标识信息和加密验证信息中的任意一个被篡改或发生扰动的情况下，得到的第一验证信息可以与验证信息明文存在区别。当对象标识信息和加密验证信息均无误时，得到的第一验证信息可以为验证信息明文。进一步地，当第一验证信息与验证信息明文不同的情况下，第一验证信息必然与第二验证信息不匹配。

根据本公开的实施例，可以在确定验证信息明文和预留验证信息相匹配的情况下，得到表示第一客户端设备完成确权的确权结果，并在确定验证信息明文和预留验证信息不匹配的情况下，得到表示第一客户端设备未完成确权的确权结果。

根据本公开的实施例，通过利用预留验证信息进行第一客户端设备的确权的方式，在便于用户记忆的同时，还可以避免数据中心化，从而保障数据安全。

根据本公开的实施例，第一区块链数据的解密过程可以在分布式私钥网络中进行。

图 4 示意性示出了根据本公开又一实施例的区块链数据处理方法的流程图。

如图 4 所示，该方法包括操作 S410~S430。

在操作 S410，响应于接收到来自第一客户端设备的数据处理请求，基于所述数据处理请求携带的对象标识信息，从第一区块链网络中获取至少一个第一区块链数据。

在操作 S420，基于数据处理请求携带的加密验证信息，对第一客户端设备进行确权。

在操作 S430，在确定第一客户端设备完成确权的情况下，向分布式私钥网络发送对象标识信息和至少一个第一区块链数据，以便分布式私钥网络根据对象标识信息，利

用至少一个第二区块链网络各自的区块体私钥，对对应的至少一个第一区块链数据进行解密，得到至少一个第二区块链数据。

根据本公开的实施例，区块体私钥可以分布式地存储在分布式私钥网络的多个分布式节点中，或者，存储在多个分布式节点的至少部分分布式节点中。每个分布式节点存储的私钥数据可以是区块体私钥的部分明文数据，也可以是利用各种加密方法得到的区块体私钥的部分密文数据，在此不作限定。每个分布式节点存储的私钥数据可以是是一个区块体私钥的部分数据，也可以包括多个区块体私钥各自的部分数据，在此不作限定。

根据本公开的实施例，通过将区块体私钥维持在分布式私钥网络中，区块体私钥不会通过明文或密文的形式单独向外部暴露，即区块体私钥不会被外部设备访问和获取，从而保障了区块链网络中数据的安全性。

下面参考图 5A~图 5B、图 6 和图 7，结合具体实施例对图 2 所示的区块链数据处理方法做进一步说明。

根据本公开的实施例，区块链数据处理平台在获取第一区块链数据或第二区块链数据之后，可以通过不落盘查看的方式在第一客户端设备上进行展示。区块链数据的不落盘查看可以包括异步数据查看、同步数据查看等方式。

图 5A 示意性示出了根据本公开实施例的区块链数据异步查看方法的示意图。

如图 5A 所示，区块链数据异步查看方法可以在请求方第一次发起数据处理请求时使用。或者，在请求方确定至少一个第二区块链网络中存在新增数据时，可以使用该区块链数据异步查看方法。

根据本公开的实施例，区块链数据处理平台 501 响应于接收到来自第一客户端设备 502 的数据处理请求 503，可以基于数据处理请求 503 携带的对象标识信息，从各个第二区块链网络 504 中跨链获取第一区块链数据 505。在确定第一客户端设备 502 完成确权后，区块链数据处理平台 501 可以向分布式私钥网络 506 发送第一区块链数据 505 和数据处理请求 503 中的对象标识信息。分布式私钥网络 506 可以根据对象标识信息，利用区块体私钥 507 对第一区块链数据 505 进行解密，得到第二区块链数据 508。分布式私钥网络 506 可以将第二区块链数据 508 返回给区块链数据处理平台 501。

根据本公开的实施例，对于每个第二区块链网络 504，区块链数据处理平台 501 可以对接收到的第二区块链数据 508 进行文本归一化处理，得到第一归一化数据 509。再对第一归一化数据 509 进行加密，得到第二归一化数据 510。区块链数据处理平台 501 可以将第二归一化数据 510 写入内存 511。

根据本公开的实施例，第一客户端设备 502 可以通过使用预设接口访问内存 511 的方式，发起数据异步查看请求。区块链数据处理平台 501 响应于检测到第一客户端设备 502 通过预设接口访问内存 511，可以向第一客户端设备 502 发送至少一个第二区块链网络 504 各自的第二归一化数据 510。第一客户端设备 502 可以针对每个第二区块链网络 504，利用与第二区块链网络 504 对应的区块体私钥 507 对第二区块链网络 504 的第二归一化数据 510 进行解密，得到第一归一化数据 509，并将第一归一化数据 509 渲染并展示在第一客户端设备 502 的显示界面 512 上。

根据本公开的实施例，文本归一化处理例如可以使用文本分类服务来实现。通过归一化处理，可以将第二区块链数据 508 中所使用各种词组进行统一。例如，对于勺子这一物品，第二区块链数据 508 中可以使用了调羹、瓢羹、瓷羹、匙羹、汤壳、饭壳、水壳等多种别名，在归一化处理后，可以将上述多种别名统一为勺子。此外，通过归一化处理，还可以对第二区块链数据 508 中设计的各类数据按预设的类型进行分类，以医疗区块链中的数据为例，可以将第二区块链数据 508 归入用户姓名、用户性别、问诊时间、疾病种类、药物类型等类别。

根据本公开的实施例，内存 511 中存储的数据可以按清理规则进行定期清理。清理规则例如可以包括按用户查看时间进行清理、按数据存储时间进行清理等。

根据本公开的实施例，在完成对请求方的数据处理请求的响应后，即在从至少一个第二区块链网络中跨链获取得到至少一个第一区块链数据的情况下，可以将至少一个第一区块链数据在第一区块链网络中上链。

图 5B 示意性示出了根据本公开实施例的区块链数据同步查看方法的示意图。

如图 5B 所示，区块链数据同步查看方法可以在请求方第二次及第二次以上发起数据处理请求时使用，即采用数据同步查看方法时，至少一个第一区块链数据可以已经记录在第一区块链网络中。或者，区块链数据同步查看方法也可以在请求方第一次发起数据处理请求的同时使用，在此不作限定。

根据本公开的实施例，区块链数据处理平台 501 响应于接收到来自第一客户端设备 502 的数据处理请求 503，可以基于数据处理请求 503 携带的对象标识信息，从第一区块链网络 513 中获取至少一个第一区块链数据 505。

根据本公开的实施例，区块链数据处理平台 501 可以将至少一个第一区块链数据 505 写入内存 511。

根据本公开的实施例，第一客户端设备 502 可以在发起数据处理请求 503 的同时，

通过预设接口访问内存 511。区块链数据处理平台 501 可以响应于检测到第一客户端设备 502 通过预设接口访问内存 511，向第一客户端设备 502 发送至少一个第二区块链网络 504 各自的第一区块链数据 505。

根据本公开的实施例，第一客户端设备 502 可以利用与至少一个第二区块链网络 504 各自对应的区块体私钥 507 对至少一个第二区块链网络 504 各自的第一区块链数据 505 进行解密，得到至少一个第二区块链数据 508，调用文本分类服务对至少一个第二区块链数据 508 进行归一化处理，得到至少一个第一归一化数据 509，并将至少一个第一归一化数据 509 渲染并展示在第一客户端设备的显示界面 512 上。

根据本公开的实施例，通过如上不落盘数据查看的方式，第二归一化数据或第一区块链数据不会写入到与区块链数据处理平台相关的磁盘中，从而可以降低数据泄露的可能性。

根据本公开的实施例，数据处理请求的请求方可以是第二区块链数据的所有方，第二区块链数据可以是由请求方在网络中生成，并由至少一个第二区块链网络搜集得到的。请求方可以对其持有的第二区块链数据进行差异化定义，实现不同数据的不同策略的处理。例如，请求方可以将其持有的第二区块链数据中的部分数据进行公开，与其他的用户进行数据共享，以获取区块链数据处理平台提供的其他服务。

图 6 示意性示出了根据本公开实施例的区块链数据共享方法的示意图。

如图 6 所示，区块链数据处理平台 501 在进行第二区块链数据 508 的展示时，可以为每条第二区块链数据 508 提供数据共享的选择项，请求方可以通过对各条第二区块链数据 508 的选择项的选择操作，确定需要进行数据共享的第二区块链数据。第一客户端设备 502 可以基于该需要进行数据共享的第二区块链数据来生成数据共享请求 601。

根据本公开的实施例，区块链数据处理平台 501 可以响应于来自第一客户端设备 502 的数据共享请求 601，获取数据共享请求 601 携带的第一目标区块链数据 602。区块链数据处理平台 501 可以对第一目标区块链数据 602 进行文本归一化处理，得到第三归一化数据 603。区块链数据处理平台 501 可以对第三归一化数据 603 进行加密，得到第四归一化数据 604。区块链数据处理平台 501 可以将第四归一化数据 604 在第三区块链网络 605 中上链。

根据本公开的实施例，对第三归一化数据 603 的加密可以利用各种加密方法来实现。各种加密方法可以包括任意的对称加密方法，如 DES（Data Encryption Standard，数据加密标准）、AES（Advanced Encryption Standard，高级加密标准）等，也可以包括任意

的非对称加密方法，如RSA、ECC（Elliptic Curve Cryptography，椭圆曲线密码）等，在此不作限定。

根据本公开的实施例，以医疗区块链为例，例如，请求方可以是亟待进行骨髓配型的病患用户，请求方的第一目标区块链数据可以是请求方的配型数据，通过将该第一目标区块链数据向外共享，可以更方便地实现骨髓配型互助。再例如，请求方的第一目标区块链数据可以是关于某项疾病的诊疗过程，该诊疗过程可以包括用药数据，通过将该第一目标区块链数据向外共享，可以作为大数据基础内容之一去指导更多的未治愈病患的用药推荐。

根据本公开的实施例，在将第四归一化数据在第三区块链网络上链后，任意用户均可对该第四归一化数据进行调用。

图7示意性示出了根据本公开实施例的区块链数据调用方法的示意图。

如图7所示，在区块链数据处理平台501将第四归一化数据604在第三区块链网络605中上链之后，区块链数据处理平台501可以响应于来自第二客户端设备701的数据调用请求702，基于数据调用请求702携带的调用类型信息，确定数据调用模型703。

根据本公开的实施例，区块链数据处理平台501可以利用数据调用模型703来处理第三区块链网络605包括的第四区块链数据704，得到第二目标区块链数据705。

根据本公开的实施例，区块链数据处理平台501可以对第二目标区块链数据705进行解密，并向第二客户端设备701发送解密后的第二目标区块链数据706。

根据本公开的实施例，数据调用模型703可以是预设算法库中的一个数据模型。预设算法库中的数据模型可以包括推荐模型、匹配模型、预测模型等，可以根据具体应用场景进行设置，在此不作限定。每个数据模型的输入端口和输出端口可以均提供给区块链数据处理平台501相应的接口，通过该接口，区块链数据处理平台501可以向数据模型输入数据，并从数据模型中提取已被数据模型处理完成的数据。

根据本公开的实施例，第四区块链数据704除可以包括由数据处理请求503的请求方提供的第四归一化数据604之外，还可以包括由其他用户共享至第三区块链网络605的区块链数据，在此不作限定。

根据本公开的实施例，以数据调用模型703为医疗区块链中的用户推荐模型为例，用户A可以通过用户推荐模型的输入接口输入用户自身的信息，例如“用户姓名”、“用户性别”、“问诊时间”、“疾病种类”、“药物类型”等属性的具体属性值，这些具体属性值可以组成用户向量A。利用用户推荐模型，可以通过基于大数据基础内容构成的数据矩

阵,与用户向量A进行相似度匹配的计算,从而通过输出接口反馈给用户A另一组由“用户姓名”、“用户性别”、“问诊时间”、“疾病种类”、“药物类型”等属性的具体属性值组成的用户向量B。用户A可以根据用户向量B中的“用户性别”等身份信息,从第三区块链网络中查询得到用户B提供的诊疗过程细节信息。或者,平台可以向用户A反馈多组用户向量,如用户向量B、用户向量C、用户向量D等,以便用户A进行选择。

作为一种可选实施方式,第二目标区块链数据705的解密可以采用与第三归一化数据603的加密时所采用的加密方法相对应的解密方法。以非对称加密为例,区块链数据处理平台501可以生成平台私钥和平台公钥。在用户进行数据共享时,区块链数据处理平台501可以使用平台私钥对共享数据进行加密,并将加密后的共享数据在第三区块链网络上链。在其他用户进行数据调用时,区块链数据处理平台501可以利用平台公钥对需要调用的数据进行解密,再将解密后的数据发送给其他用户。或者,区块链数据处理平台501也可以向有权进行数据调用的用户提供平台公钥,在该用户进行数据调用时,区块链数据处理平台501可以直接将第三区块链网络中的待调用数据发送给该用户,由该用户使用平台公钥对待调用数据进行解密。

图8示意性示出了根据本公开实施例的区块链数据处理平台的示意图。

如图8所示,区块链数据处理平台501可以包括区块链数据源管理模块5011、私钥控制模块5012和数据处理模块5013。

区块链数据源管理模块5011,被配置为响应于接收到来自第一客户端设备的数据处理请求,基于数据处理请求携带的对象标识信息,从第一区块链网络中获取至少一个第一区块链数据。

私钥控制模块5012,被配置为基于数据处理请求携带的加密验证信息,对第一客户端设备进行确权。

数据处理模块5013,被配置为在确定第一客户端设备完成确权的情况下,向第一客户端设备发送至少一个第一区块链数据,以便第一客户端设备利用与至少一个第一区块链数据各自对应的区块体私钥,对至少一个第一区块链数据进行解密,得到至少一个第二区块链数据。

根据本公开的实施例,加密验证信息是由第一客户端设备利用对象私钥对私钥摘要信息进行数字签名而得到的,私钥摘要信息是由第一客户端设备对与至少一个第一区块链数据各自对应的区块体私钥进行拼接和哈希计算而得到的。

根据本公开的实施例,私钥控制模块5012被配置为:基于对象标识信息,得到对

象公钥，其中，对象公钥与对象私钥相对应。利用对象公钥对加密验证信息进行验签，得到第一摘要信息，其中，在加密验证信息验签成功的情况下，第一摘要信息为私钥摘要信息。向分布式私钥网络发送对象标识信息和第一摘要信息，以便分布式私钥网络根据对象标识信息，确定至少一个区块链体私钥，对至少一个区块体私钥进行拼接和哈希计算，得到第二摘要信息，并基于第一摘要信息和第二摘要信息的匹配结果，确定第一客户端设备的确权结果。

根据本公开的实施例，区块链数据源管理模块 5011 被配置为：响应于数据处理请求，在未能从第一区块链网络中获取至少一个第一区块链数据的情况下，基于对象标识信息，分别对至少一个第二区块链网络进行跨链数据获取，得到至少一个第一区块链数据。

根据本公开的实施例，区块链数据源管理模块 5011 被配置为：对于每个第二区块链网络，确定第二区块链网络的跨链节点。基于跨链节点的节点类型，通过跨链节点来获取第一区块链数据。

根据本公开的实施例，区块链数据源管理模块 5011 被配置为：在确定跨链节点为全节点的情况下，向跨链节点发送包括对象标识信息的数据获取请求，以便基于跨链节点返回的第一反馈数据，得到第一区块链数据。其中，第一反馈数据是由跨链节点基于对象标识信息，从跨链节点的账本中得到的。

根据本公开的实施例，区块链数据源管理模块 5011 被配置为：在确定跨链节点为轻节点的情况下，通过跨链节点向第二区块链网络的全节点发送包括对象标识信息的数据获取请求，以便基于全节点通过跨链节点返回的第二反馈数据，得到第一区块链数据。其中，第二反馈数据是由全节点基于由跨链节点转发的对象标识信息，从全节点的账本中得到的。

根据本公开的实施例，区块链数据源管理模块 5011 被配置为：对于每个第二区块链网络，在第二区块链网络为公有链网络的情况下，向第二区块链网络包括的多个区块链节点广播包括对象标识信息的数据获取请求。基于多个区块链节点各自返回的第三反馈数据，得到第一区块链数据，其中，第三反馈数据是由区块链节点基于对象标识信息，从区块链节点的账本中得到的。

根据本公开的实施例，加密验证信息是由第一客户端设备利用对象私钥对验证信息明文进行数字签名而得到的，验证信息明文是由第一客户端设备对加密组合信息进行哈希计算得到的。

根据本公开的实施例，私钥控制模块 5012 被配置为：基于对象标识信息，得到预留加密组合信息和对象公钥，其中，对象公钥与对象私钥相对应。利用对象公钥对加密验证信息进行验签，得到第一验证信息，其中，在确定加密验证信息验签成功的情况下，第一验证信息为验证信息明文。对预留加密组合信息进行哈希计算，得到第二验证信息。基于第一验证信息和第二验证信息的匹配结果，确定第一客户端设备的确权结果。

根据本公开的实施例，加密组合信息或预留加密组合信息包括以下至少一项：预设问题的答案文本，密码字符串，生物特征信息。

根据本公开的实施例，私钥控制模块 5012 被配置为：在确定第一客户端设备完成确权的情况下，向分布式私钥网络发送对象标识信息和至少一个第一区块链数据，以便分布式私钥网络根据对象标识信息，利用至少一个第二区块链网络各自的区块体私钥，对对应的至少一个第一区块链数据进行解密，得到至少一个第二区块链数据。

根据本公开的实施例，数据处理模块 5013 被配置为：对于每个第二区块链网络，对第二区块链网络的第二区块链数据进行文本归一化处理，得到第一归一化数据。利用与第二区块链网络对应的区块体公钥对第一归一化数据进行加密，得到第二归一化数据，其中，区块体公钥与区块体私钥相对应。将第二归一化数据写入内存。响应于检测到第一客户端设备通过预设接口访问内存，向第一客户端设备发送至少一个第二区块链网络各自的第二归一化数据，其中，第一客户端设备被配置为针对每个第二区块链网络，利用与第二区块链网络对应的区块体私钥对第二区块链网络的第二归一化数据进行解密，得到第一归一化数据，并将第一归一化数据渲染并展示在第一客户端设备的显示界面上。

根据本公开的实施例，数据处理模块 5013 被配置为：在从至少一个第二区块链网络中跨链获取得到至少一个第一区块链数据的情况下，将至少一个第一区块链数据在第一区块链网络中上链。

根据本公开的实施例，数据处理模块 5013 被配置为：将至少一个第一区块链数据写入内存。响应于检测到第一客户端设备通过预设接口访问内存，向第一客户端设备发送至少一个第一区块链数据，其中，第一客户端设备被配置为利用与至少一个第一区块链数据各自对应的区块体私钥，对至少一个第一区块链数据进行解密，得到至少一个第二区块链数据，调用文本分类服务对至少一个第二区块链数据进行归一化处理，得到至少一个第一归一化数据，并将至少一个第一归一化数据渲染并展示在第一客户端设备的显示界面上。

根据本公开的实施例，数据处理模块 5013 被配置为：响应于来自第一客户端设备

的数据共享请求，获取数据共享请求携带的第一目标区块链数据。对第一目标区块链数据进行文本归一化处理，得到第三归一化数据。对第三归一化数据进行加密，得到第四归一化数据。将第四归一化数据在第三区块链网络中上链。

根据本公开的实施例，数据处理模块 5013 被配置为：响应于来自第二客户端设备的数据调用请求，基于数据调用请求携带的调用类型信息，确定数据调用模型。利用数据调用模型来处理第三区块链网络包括的第四区块链数据，得到第二目标区块链数据，其中，第四区块链数据包括第四归一化数据。对第二目标区块链数据进行解密，并向第二客户端设备发送解密后的第二目标区块链数据。

需要说明的是，本公开的实施例中区块链数据处理平台部分与本公开的实施例中区块链数据处理方法部分是相对应的，区块链数据处理平台部分的描述具体参考区块链数据处理方法部分，在此不再赘述。

图 9 示意性示出了根据本公开实施例的区块链数据处理系统的示意图。

如图 9 所示，区块链数据处理系统可以包括第一客户端设备 502、第一区块链网络 513、区块链数据处理平台 501 和分布式私钥网络 506。

其中，区块链数据处理平台 501 被配置为：响应于接收到来自第一客户端设备的数据处理请求，基于数据处理请求携带的对象标识信息，从第一区块链网络中获取至少一个第一区块链数据。基于数据处理请求携带的加密验证信息，对第一客户端设备进行确权。在确定第一客户端设备完成确权的情况下，向第一客户端设备发送至少一个第一区块链数据。

第一客户端设备 502 被配置为：利用与至少一个第一区块链数据各自对应的区块体私钥，对至少一个第一区块链数据进行解密，得到至少一个第二区块链数据。

根据本公开的实施例，区块链数据处理系统还可以包括至少一个第二区块链网络 504。

根据本公开的实施例，区块链数据处理平台 501 可以被配置为：响应于数据处理请求，在未能从第一区块链网络中获取至少一个第一区块链数据的情况下，基于对象标识信息，分别对至少一个第二区块链网络进行跨链数据获取，得到至少一个第一区块链数据。

根据本公开的实施例，区块链数据处理平台 501 可以被配置为：在确定第一客户端设备完成确权的情况下，向分布式私钥网络发送对象标识信息和至少一个第一区块链数据。

根据本公开的实施例，分布式私钥网络506可以被配置为：根据对象标识信息，利用至少一个第二区块链网络各自的区块体私钥，对对应的至少一个第一区块链数据进行解密，得到至少一个第二区块链数据。

根据本公开的实施例，分布式私钥网络506可以被配置为：响应于接收到来自区块链数据处理平台的对象标识信息和至少一个第一区块链数据，基于对象标识信息，从多个分布式节点中确定至少一个目标节点。基于至少一个目标节点各自存储的私钥数据，得到至少一个第二区块链网络各自的区块体私钥。利用至少一个第二区块链网络各自的区块体私钥，对对应的至少一个第一区块链数据进行解密，得到至少一个第二区块链数据。向区块链数据处理平台发送至少一个第二区块链数据。

根据本公开的实施例，目标节点存储的私钥数据为字符串数据。

根据本公开的实施例，分布式私钥网络506可以被配置为：对于每个目标节点，基于目标节点存储的私钥数据，得到拼接顺序信息和目标字符串数据。基于至少一个目标节点各自的拼接顺序信息，将至少一个目标节点各自的目标字符串数据进行拼接，得到目标区块体私钥。基于区块体私钥的预设字符长度，对目标区块体私钥进行切分，得到至少一个第二区块链网络各自的区块体私钥。

根据本公开的实施例，分布式私钥网络在将属于同一请求方的至少一个区块体私钥进行存储时，可以先将至少一个区块体私钥进行拼接，得到目标区块体私钥。或者，也可以对拼接后的至少一个区块体私钥进行进一步的加密处理，以得到目标区块体私钥。可以将目标区块体私钥切分为多份，根据切分的份数，可以从多个分布式节点中确定相应数量的目标节点，并在每个目标节点中生成与目标区块体私钥具有相同尺寸的字符串型参数，该字符串型参数的参数值可以为空。在进行目标区块体私钥的存储分配时，可以基于每一份切分后的目标区块体私钥在原区块体私钥中的位置，对目标节点的字符串型参数中相应位置的元素进行替换，得到私钥数据，从而实现该部分的目标区块体私钥在目标节点的存储。

根据本公开的实施例，在获取区块体私钥时，对于每个目标节点，分布式私钥网络可以基于目标节点存储的私钥数据，得到拼接顺序信息和目标字符串数据。具体地，可以基于各个私钥数据中非空字符串数据所处的位置，来得到拼接顺序信息。目标字符串数据可以为私钥数据中的非空字符串数据。

根据本公开的实施例，分布式私钥网络可以基于至少一个目标节点各自的拼接顺序信息，将至少一个目标节点各自的目标字符串数据进行拼接，得到目标区块体私钥。

根据本公开的实施例，由于至少一个区块体私钥均可以是使用相同位数的加密算法来生成的，因此可以基于区块体私钥的预设字符长度，对目标区块体私钥进行切分，得到至少一个区块链网络各自的区块体私钥。

根据本公开的实施例，至少一个区块体私钥的位数可以不相同。可以在生成目标区块体私钥的过程中，记录各个区块体私钥拼接顺序及位数，并可以基于该记录实现对目标区块体私钥的切分。

根据本公开的实施例，目标节点存储的私钥数据可以为曲线坐标数据。

根据本公开的实施例，分布式私钥网络306可以被配置为：基于曲线模板，对至少一个目标节点各自存储的私钥数据进行曲线拟合，得到目标曲线。将目标曲线包括的多个参数值进行拼接，得到目标区块体私钥。基于区块体私钥的预设字符长度，对目标区块体私钥进行切分，得到至少一个第二区块链网络各自的区块体私钥。

根据本公开的实施例，分布式私钥网络在将属于同一请求方的至少一个区块体私钥进行存储时，可以先将至少一个区块体私钥进行拼接，并将拼接后的至少一个区块体私钥进一步地处理为一个整数数值。可以根据该整数数值的位数，选择一个曲线模板，按曲线模板中各个参数的规定位数，将该整数数值拆分为多个参数值，并将多个参数值赋予曲线模板的各个参数，以得到目标曲线。例如，该整数值可以为12345678，选择的曲线模板可以表示为 $y=ax^2+bx^2+cx+d$，每个参数的规定位数可以均为2位，则曲线模板的参数可以分别赋值为 a=12、b=34、c=56、d=78。在完成赋值后，得到的目标曲线可以表示为 $y=12x^2+23x^2+56x+78$。在确定目标曲线后，可以随机从该目标曲线上选择多个坐标点，选择的坐标点的数量可以大于或等于曲线模板中参数的数量。可以基于坐标点的数量，从多个分布式节点中选择相应数量的目标节点，并将多个坐标点的曲线坐标数据写入到各个目标节点中。

根据本公开的实施例，在获取区块体私钥时，分布式私钥网络可以基于曲线模板，对至少一个目标节点各自存储的私钥数据进行曲线拟合，得到目标曲线。可以将目标曲线包括的多个参数值进行拼接，得到目标区块体私钥。可以基于区块体私钥的预设字符长度，对目标区块体私钥进行切分，得到至少一个区块链网络各自的区块体私钥。

根据本公开的实施例，通过利用分布式节点来分布式地存储区块体私钥的方式，可以规避信息存储的单点风险，有助于保障用户的区块体私钥的隐私安全，从而间接地保护用户的区块链数据的私密性和安全性。

根据本公开的实施例，区块链数据处理系统包括的第一客户端设备、第一区块链网

络、至少一个第二区块链网络、区块链数据处理平台和分布式私钥网络可以用于实现本公开实施例所述的区块链数据处理方法，可以参考上文相应部分的说明，在此不再赘述。

图 10 示意性示出了根据本公开实施例的区块链数据处理装置的框图。

如图 10 所示，区块链数据处理装置 1000 可以包括第一获取模块 1010、确权模块 1020 和第一发送模块 1030。

第一获取模块 1010，用于响应于接收到来自第一客户端设备的数据处理请求，基于数据处理请求携带的对象标识信息，从第一区块链网络中获取至少一个第一区块链数据。

确权模块 1020，用于基于数据处理请求携带的加密验证信息，对第一客户端设备进行确权。

第一发送模块 1030，用于在确定第一客户端设备完成确权的情况下，向第一客户端设备发送至少一个第一区块链数据，以便第一客户端设备利用与至少一个第一区块链数据各自对应的区块体私钥，对至少一个第一区块链数据进行解密，得到至少一个第二区块链数据。

根据本公开的实施例，加密验证信息是由第一客户端设备利用对象私钥对私钥摘要信息进行数字签名而得到的，私钥摘要信息是由第一客户端设备对与至少一个第一区块链数据各自对应的区块体私钥进行拼接和哈希计算而得到的。

根据本公开的实施例，确权模块 1020 包括第一确权单元、第二确权单元和第三确权单元。

第一确权单元，用于基于对象标识信息，得到对象公钥，其中，对象公钥与对象私钥相对应。

第二确权单元，用于利用对象公钥对加密验证信息进行验签，得到第一摘要信息，其中，在加密验证信息验签成功的情况下，第一摘要信息为私钥摘要信息。

第三确权单元，用于向分布式私钥网络发送对象标识信息和第一摘要信息，以便分布式私钥网络根据对象标识信息，确定至少一个区块链体私钥，对至少一个区块体私钥进行拼接和哈希计算，得到第二摘要信息，并基于第一摘要信息和第二摘要信息的匹配结果，确定第一客户端设备的确权结果。

根据本公开的实施例，区块链数据处理装置 1000 还包括第二获取模块。

第二获取模块，用于响应于数据处理请求，在未能从第一区块链网络中获取至少一个第一区块链数据的情况下，基于对象标识信息，分别对至少一个第二区块链网络进行跨链数据获取，得到至少一个第一区块链数据。

根据本公开的实施例，第二获取模块包括第一获取单元和第二获取单元。

第一获取单元，用于对于每个第二区块链网络，确定第二区块链网络的跨链节点。

第二获取单元，用于基于跨链节点的节点类型，通过跨链节点来获取第一区块链数据。

根据本公开的实施例，第二获取单元包括第一获取子单元。

第一获取子单元，用于在确定跨链节点为全节点的情况下，向跨链节点发送包括对象标识信息的数据获取请求，以便基于跨链节点返回的第一反馈数据，得到第一区块链数据。其中，第一反馈数据是由跨链节点基于对象标识信息，从跨链节点的账本中得到的。

根据本公开的实施例，第二获取单元包括第二获取子单元。

第二获取子单元，用于在确定跨链节点为轻节点的情况下，通过跨链节点向第二区块链网络的全节点发送包括对象标识信息的数据获取请求，以便基于全节点通过跨链节点返回的第二反馈数据，得到第一区块链数据。其中，第二反馈数据是由全节点基于由跨链节点转发的对象标识信息，从全节点的账本中得到的。

根据本公开的实施例，第二获取模块包括第三获取单元和第四获取单元。

第三获取单元，用于对于每个第二区块链网络，在第二区块链网络为公有链网络的情况下，向第二区块链网络包括的多个区块链节点广播包括对象标识信息的数据获取请求。

第四获取单元，用于基于多个区块链节点各自返回的第三反馈数据，得到第一区块链数据，其中，第三反馈数据是由区块链节点基于对象标识信息，从区块链节点的账本中得到的。

根据本公开的实施例，加密验证信息是由第一客户端设备利用对象私钥对验证信息明文进行数字签名而得到的，验证信息明文是由第一客户端设备对加密组合信息进行哈希计算得到的。

根据本公开的实施例，确权模块 1020 包括第四确权单元、第五确权单元、第六确权单元和第七确权单元。

第四确权单元，用于基于对象标识信息，得到预留加密组合信息和对象公钥，其中，对象公钥与对象私钥相对应。

第五确权单元，用于利用对象公钥对加密验证信息进行验签，得到第一验证信息，其中，在确定加密验证信息验签成功的情况下，第一验证信息为验证信息明文。

第六确权单元，用于对预留加密组合信息进行哈希计算，得到第二验证信息。

第七确权单元，用于基于第一验证信息和第二验证信息的匹配结果，确定第一客户端设备的确权结果。

根据本公开的实施例，加密组合信息或预留加密组合信息包括以下至少一项：预设问题的答案文本，密码字符串，生物特征信息。

根据本公开的实施例，区块链数据处理装置1000还包括第二发送模块。

第二发送模块，用于在确定第一客户端设备完成确权的情况下，向分布式私钥网络发送对象标识信息和至少一个第一区块链数据，以便分布式私钥网络根据对象标识信息，利用至少一个第二区块链网络各自的区块体私钥，对对应的至少一个第一区块链数据进行解密，得到至少一个第二区块链数据。

根据本公开的实施例，区块链数据处理装置1000还包括第一处理模块、第一加密模块、第一写入模块和第三发送模块。

第一处理模块，用于对于每个第二区块链网络，对第二区块链网络的第二区块链数据进行文本归一化处理，得到第一归一化数据。

第一加密模块，用于利用与第二区块链网络对应的区块体公钥对第一归一化数据进行加密，得到第二归一化数据，其中，区块体公钥与区块体私钥相对应。

第一写入模块，用于将第二归一化数据写入内存。

第三发送模块，用于响应于检测到第一客户端设备通过预设接口访问内存，向第一客户端设备发送至少一个第二区块链网络各自的第二归一化数据，其中，第一客户端设备被配置为针对每个第二区块链网络，利用与第二区块链网络对应的区块体私钥对第二区块链网络的第二归一化数据进行解密，得到第一归一化数据，并将第一归一化数据渲染并展示在第一客户端设备的显示界面上。

根据本公开的实施例，区块链数据处理装置1000还包括第一上链模块。

第一上链模块，用于在从至少一个第二区块链网络中跨链获取得到至少一个第一区块链数据的情况下，将至少一个第一区块链数据在第一区块链网络中上链。

根据本公开的实施例，区块链数据处理装置1000还包括第二写入模块和第四发送模块。

第二写入模块，用于将至少一个第一区块链数据写入内存。

第四发送模块，用于响应于检测到第一客户端设备通过预设接口访问内存，向第一客户端设备发送至少一个第一区块链数据，其中，第一客户端设备被配置为利用与至少

一个第一区块链数据各自对应的区块体私钥，对至少一个第一区块链数据进行解密，得到至少一个第二区块链数据，调用文本分类服务对至少一个第二区块链数据进行归一化处理，得到至少一个第一归一化数据，并将至少一个第一归一化数据渲染并展示在第一客户端设备的显示界面上。

根据本公开的实施例，区块链数据处理装置 1000 还包括第三获取模块、第二处理模块、第二加密模块和第二上链模块。

第三获取模块，用于响应于来自第一客户端设备的数据共享请求，获取数据共享请求携带的第一目标区块链数据。

第二处理模块，用于对第一目标区块链数据进行文本归一化处理，得到第三归一化数据。

第二加密模块，用于对第三归一化数据进行加密，得到第四归一化数据。

第二上链模块，用于将第四归一化数据在第三区块链网络中上链。

根据本公开的实施例，区块链数据处理装置 1000 还包括确定模块、第三处理模块和第五发送模块。

确定模块，用于响应于来自第二客户端设备的数据调用请求，基于数据调用请求携带的调用类型信息，确定数据调用模型。

第三处理模块，用于利用数据调用模型来处理第三区块链网络包括的第四区块链数据，得到第二目标区块链数据，其中，第四区块链数据包括第四归一化数据。

第五发送模块，用于对第二目标区块链数据进行解密，并向第二客户端设备发送解密后的第二目标区块链数据。

根据本公开的实施例的模块、子模块、单元、子单元中的任意多个、或其中任意多个的至少部分功能可以在一个模块中实现。根据本公开实施例的模块、子模块、单元、子单元中的任意一个或多个可以被拆分成多个模块来实现。根据本公开实施例的模块、子模块、单元、子单元中的任意一个或多个可以至少被部分地实现为硬件电路，例如现场可编程门阵列（Field Programmable Gate Array ，FPGA）、可编程逻辑阵列（Programmable Logic Arrays ，PLA）、片上系统、基板上的系统、封装上的系统、专用集成电路（Application Specific Integrated Circuit ，ASIC），或可以通过对电路进行集成或封装的任何其他的合理方式的硬件或固件来实现，或以软件、硬件以及固件三种实现方式中任意一种或以其中任意几种的适当组合来实现。或者，根据本公开实施例的模块、子模块、单元、子单元中的一个或多个可以至少被部分地实现为计算机程序模块，

当该计算机程序模块被运行时，可以执行相应的功能。

例如，第一获取模块 1010、确权模块 1020 和第一发送模块 1030 中的任意多个可以合并在一个模块/单元/子单元中实现，或者其中的任意一个模块/单元/子单元可以被拆分成多个模块/单元/子单元。或者，这些模块/单元/子单元中的一个或多个模块/单元/子单元的至少部分功能可以与其他模块/单元/子单元的至少部分功能相结合，并在一个模块/单元/子单元中实现。根据本公开的实施例，第一获取模块 1010、确权模块 1020 和第一发送模块 1030 中的至少一个可以至少被部分地实现为硬件电路，例如现场可编程门阵列（FPGA）、可编程逻辑阵列（PLA）、片上系统、基板上的系统、封装上的系统、专用集成电路（ASIC），或可以通过对电路进行集成或封装的任何其他的合理方式等硬件或固件来实现，或以软件、硬件以及固件三种实现方式中任意一种或以其中任意几种的适当组合来实现。或者，第一获取模块 1010、确权模块 1020 和第一发送模块 1030 中的至少一个可以至少被部分地实现为计算机程序模块，当该计算机程序模块被运行时，可以执行相应的功能。

需要说明的是，本公开的实施例中区块链数据处理装置部分与本公开的实施例中区块链数据处理方法部分是相对应的，区块链数据处理装置部分的描述具体参考区块链数据处理方法部分，在此不再赘述。

图 11 示意性示出了根据本公开实施例的适于实现区块链数据处理方法的电子设备的框图。图 11 示出的电子设备仅仅是一个示例，不应对本公开实施例的功能和使用范围带来任何限制。

如图 11 所示，根据本公开实施例的电子设备 1100 包括处理器 1101，其可以根据存储在只读存储器（Read-Only Memory，ROM）1102 中的程序或者从存储部分 1108 加载到随机访问存储器（Random Access Memory，RAM）1103 中的程序而执行各种适当的动作和处理。处理器 1101 例如可以包括通用微处理器（例如 CPU）、指令集处理器和/或相关芯片组和/或专用微处理器（例如，专用集成电路（ASIC）），等等。处理器 1101 还可以包括用于缓存用途的板载存储器。处理器 1101 可以包括用于执行根据本公开实施例的方法流程的不同动作的单一处理单元或者是多个处理单元。

在 RAM 1103 中，存储有电子设备 1100 操作所需的各种程序和数据。处理器 1101、ROM 1102 以及 RAM 1103 通过总线 1104 彼此相连。处理器 1101 通过执行 ROM 1102 和/或 RAM 1103 中的程序来执行根据本公开实施例的方法流程的各种操作。需要注意，所述程序也可以存储在除 ROM 1102 和 RAM 1103 以外的一个或多个存储器中。处理器

1101 也可以通过执行存储在所述一个或多个存储器中的程序来执行根据本公开实施例的方法流程的各种操作。

根据本公开的实施例，电子设备 1100 还可以包括输入/输出（I/O）接口 1105，输入/输出（I/O）接口 1105 也连接至总线 1104。系统 1100 还可以包括连接至 I/O 接口 1105 的以下部件中的一项或多项：包括键盘、鼠标等的输入部分 1106；包括诸如阴极射线管（CRT）、液晶显示器（Liquid Crystal Display，LCD）等以及扬声器等的输出部分 1107；包括硬盘等的存储部分 1108；以及包括诸如 LAN 卡、调制解调器等的网络接口卡的通信部分 1109。通信部分 1109 经由诸如因特网的网络执行通信处理。驱动器 1110 也根据需要连接至 I/O 接口 1105。可拆卸介质 1111，诸如磁盘、光盘、磁光盘、半导体存储器等等，根据需要安装在驱动器 1110 上，以便于从其上读出的计算机程序根据需要被安装入存储部分 1108。

根据本公开的实施例，根据本公开实施例的方法流程可以被实现为计算机软件程序。例如，本公开的实施例包括一种计算机程序产品，其包括承载在计算机可读存储介质上的计算机程序，该计算机程序包含用于执行流程图所示的方法的程序代码。在这样的实施例中，该计算机程序可以通过通信部分 1109 从网络上被下载和安装，和/或从可拆卸介质 1111 被安装。在该计算机程序被处理器 1101 执行时，执行本公开实施例的系统中限定的上述功能。根据本公开的实施例，上文描述的系统、设备、装置、模块、单元等可以通过计算机程序模块来实现。

本公开还提供了一种计算机可读存储介质，该计算机可读存储介质可以是上述实施例中描述的设备/装置/系统中所包含的；也可以是单独存在，而未装配入该设备/装置/系统中。上述计算机可读存储介质承载有一个或者多个程序，当上述一个或者多个程序被执行时，实现根据本公开实施例的方法。

根据本公开的实施例，计算机可读存储介质可以是非易失性的计算机可读存储介质。例如可以包括但不限于：便携式计算机磁盘、硬盘、随机访问存储器（RAM）、只读存储器（ROM）、可擦式可编程只读存储器（EPROM（Erasable Programmable Read Only Memory，EPROM）或闪存）、便携式紧凑磁盘只读存储器（Computer Disc Read-Only Memory，CD-ROM）、光存储器件、磁存储器件、或者上述的任意合适的组合。在本公开中，计算机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。

例如，根据本公开的实施例，计算机可读存储介质可以包括上文描述的 ROM 1102

和/或 RAM 1103 和/或 ROM 1102 和 RAM 1103 以外的一个或多个存储器。

本公开的实施例还包括一种计算机程序产品，其包括计算机程序，该计算机程序包含用于执行本公开实施例所提供的方法的程序代码，当计算机程序产品在电子设备上运行时，该程序代码用于使电子设备实现本公开实施例所提供的区块链数据处理方法。

在该计算机程序被处理器 1101 执行时，执行本公开实施例的系统/装置中限定的上述功能。根据本公开的实施例，上文描述的系统、装置、模块、单元等可以通过计算机程序模块来实现。

在一种实施例中，该计算机程序可以依托于光存储器件、磁存储器件等有形存储介质。在另一种实施例中，该计算机程序也可以在网络介质上以信号的形式进行传输、分发，并通过通信部分 1109 被下载和安装，和/或从可拆卸介质 1111 被安装。该计算机程序包含的程序代码可以用任何适当的网络介质传输，包括但不限于：无线、有线等等，或者上述的任意合适的组合。

根据本公开的实施例，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公开实施例提供的计算机程序的程序代码，具体地，可以利用高级过程和/或面向对象的编程语言、和/或汇编/机器语言来实施这些计算程序。程序设计语言包括但不限于诸如 Java，C++，Python，“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、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（Local Area Network，LAN）或广域网（Wide Area Networks ，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）。

附图中的流程图和框图，图示了按照本公开各种实施例的系统、方法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上，流程图或框图中的每个方框可以代表一个模块、程序段、或代码的一部分，上述模块、程序段、或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。也应当注意，在有些作为替换的实现中，方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如，两个接连地表示的方框实际上可以基本并行地执行，它们有时也可以按相反的顺序执行，这依所涉及的功能而定。也要注意的是，框图或流程图中的每个方框、以及框图或流程图中的方框的组合，可以用执行规定的功能或操作的专用的基于硬件的系统来实现，或者可以用专用硬件与计算机指令的组合来实现。本领域技术人员可以理解，本公开的各个实施例

和/或权利要求中记载的特征可以进行多种组合和/或结合，即使这样的组合或结合没有明确记载于本公开中。特别地，在不脱离本公开精神和教导的情况下，本公开的各个实施例和/或权利要求中记载的特征可以进行多种组合和/或结合。所有这些组合和/或结合均落入本公开的范围。

以上对本公开的实施例进行了描述。但是，这些实施例仅仅是为了说明的目的，而并非为了限制本公开的范围。尽管在以上分别描述了各实施例，但是这并不意味着各个实施例中的措施不能有利地结合使用。本公开的范围由所附权利要求及其等同物限定。不脱离本公开的范围，本领域技术人员可以做出多种替代和修改，这些替代和修改都应落在本公开的范围之内。

权 利 要 求

1．一种区块链数据处理方法，包括：

响应于接收到来自第一客户端设备的数据处理请求，基于所述数据处理请求携带的对象标识信息，从第一区块链网络中获取至少一个第一区块链数据；

基于所述数据处理请求携带的加密验证信息，对所述第一客户端设备进行确权；以及

在确定所述第一客户端设备完成确权的情况下，向所述第一客户端设备发送所述至少一个第一区块链数据，以便所述第一客户端设备利用与所述至少一个第一区块链数据各自对应的区块体私钥，对所述至少一个第一区块链数据进行解密，得到至少一个第二区块链数据。

2．根据权利要求1所述的方法，其中，所述加密验证信息是由第一客户端设备利用对象私钥对私钥摘要信息进行数字签名而得到的，所述私钥摘要信息是由第一客户端设备对与所述至少一个第一区块链数据各自对应的区块体私钥进行拼接和哈希计算而得到的；

其中，所述基于所述数据处理请求携带的加密验证信息，对所述第一客户端设备进行确权，包括：

基于所述对象标识信息，得到对象公钥，其中，所述对象公钥与所述对象私钥相对应；

利用所述对象公钥对所述加密验证信息进行验签，得到第一摘要信息，其中，在所述加密验证信息验签成功的情况下，所述第一摘要信息为所述私钥摘要信息；以及

向分布式私钥网络发送所述对象标识信息和所述第一摘要信息，以便所述分布式私钥网络根据所述对象标识信息，确定至少一个区块链体私钥，对所述至少一个区块体私钥进行拼接和哈希计算，得到第二摘要信息，并基于所述第一摘要信息和所述第二摘要信息的匹配结果，确定所述第一客户端设备的确权结果。

3．根据权利要求1所述的方法，还包括：

响应于所述数据处理请求，在未能从所述第一区块链网络中获取所述至少一个第一区块链数据的情况下，基于所述对象标识信息，分别对至少一个第二区块链网络进行跨链数据获取，得到所述至少一个第一区块链数据。

4．根据权利要求3所述的方法，其中，所述基于所述对象标识信息，分别对至少一个第二区块链网络进行跨链数据获取，得到所述至少一个第一区块链数据，包括：

对于每个所述第二区块链网络，确定所述第二区块链网络的跨链节点；以及

基于所述跨链节点的节点类型，通过所述跨链节点来获取所述第一区块链数据。

5．根据权利要求4所述的方法，其中，所述基于所述跨链节点的节点类型，通过所述跨链节点来获取所述第一区块链数据，包括：

在确定所述跨链节点为全节点的情况下，向所述跨链节点发送包括所述对象标识信息的数据获取请求，以便基于所述跨链节点返回的第一反馈数据，得到所述第一区块链数据；

其中，所述第一反馈数据是由所述跨链节点基于所述对象标识信息，从所述跨链节点的账本中得到的。

6．根据权利要求4所述的方法，其中，所述基于所述跨链节点的节点类型，通过所述跨链节点来获取所述第一区块链数据，包括：

在确定所述跨链节点为轻节点的情况下，通过所述跨链节点向所述第二区块链网络的全节点发送包括所述对象标识信息的数据获取请求，以便基于所述全节点通过所述跨链节点返回的第二反馈数据，得到所述第一区块链数据；

其中，所述第二反馈数据是由所述全节点基于由所述跨链节点转发的所述对象标识信息，从所述全节点的账本中得到的。

7．根据权利要求3所述的方法，其中，所述基于所述对象标识信息，分别对至少一个第二区块链网络进行跨链数据获取，得到所述至少一个第一区块链数据，包括：

对于每个所述第二区块链网络，在所述第二区块链网络为公有链网络的情况下，向所述第二区块链网络包括的多个区块链节点广播包括所述对象标识信息的数据获取请求；以及

基于所述多个区块链节点各自返回的第三反馈数据，得到所述第一区块链数据，其中，所述第三反馈数据是由所述区块链节点基于所述对象标识信息，从所述区块链节点的账本中得到的。

8．根据权利要求3所述的方法，其中，所述加密验证信息是由第一客户端设备利用对象私钥对验证信息明文进行数字签名而得到的，所述验证信息明文是由所述第一客户端设备对加密组合信息进行哈希计算得到的；

其中，所述基于所述数据处理请求携带的加密验证信息，对所述第一客户端设备进行确权，包括：

基于所述对象标识信息，得到预留加密组合信息和对象公钥，其中，所述对象公

钥与所述对象私钥相对应；

利用所述对象公钥对所述加密验证信息进行验签，得到第一验证信息，其中，在确定所述加密验证信息验签成功的情况下，所述第一验证信息为所述验证信息明文；

对所述预留加密组合信息进行哈希计算，得到第二验证信息；以及

基于所述第一验证信息和所述第二验证信息的匹配结果，确定所述第一客户端设备的确权结果。

9．根据权利要求 8 所述的方法，其中，所述加密组合信息或所述预留加密组合信息包括以下至少一项：

预设问题的答案文本，密码字符串，生物特征信息。

10．根据权利要求 1 所述的方法，还包括：

在确定所述第一客户端设备完成确权的情况下，向分布式私钥网络发送所述对象标识信息和至少一个所述第一区块链数据，以便所述分布式私钥网络根据所述对象标识信息，利用所述至少一个第二区块链网络各自的区块体私钥，对对应的至少一个所述第一区块链数据进行解密，得到至少一个第二区块链数据。

11．根据权利要求 10 所述的方法，还包括：

对于每个所述第二区块链网络，对所述第二区块链网络的第二区块链数据进行文本归一化处理，得到第一归一化数据；

利用与所述第二区块链网络对应的区块体公钥对所述第一归一化数据进行加密，得到第二归一化数据，其中，所述区块体公钥与所述区块体私钥相对应；

将所述第二归一化数据写入内存；以及

响应于检测到所述第一客户端设备通过预设接口访问所述内存，向所述第一客户端设备发送所述至少一个第二区块链网络各自的第二归一化数据，其中，所述第一客户端设备被配置为针对每个第二区块链网络，利用与所述第二区块链网络对应的区块体私钥对所述第二区块链网络的第二归一化数据进行解密，得到所述第一归一化数据，并将所述第一归一化数据渲染并展示在所述第一客户端设备的显示界面上。

12．根据权利要求 1~11 中任一项所述的方法，还包括：

在从所述至少一个第二区块链网络中跨链获取得到所述至少一个第一区块链数据的情况下，将所述至少一个第一区块链数据在所述第一区块链网络中上链。

13．根据权利要求 1~11 中任一项所述的方法，还包括：

将所述至少一个第一区块链数据写入内存；以及

响应于检测到所述第一客户端设备通过预设接口访问所述内存，向所述第一客户端设备发送所述至少一个第一区块链数据，其中，所述第一客户端设备被配置为利用与所述至少一个第一区块链数据各自对应的区块体私钥，对所述至少一个第一区块链数据进行解密，得到至少一个第二区块链数据，调用文本分类服务对所述至少一个第二区块链数据进行归一化处理，得到至少一个第一归一化数据，并将所述至少一个第一归一化数据渲染并展示在所述第一客户端设备的显示界面上。

14．根据权利要求1~11中任一项所述的方法，还包括：

响应于来自所述第一客户端设备的数据共享请求，获取所述数据共享请求携带的第一目标区块链数据；

对所述第一目标区块链数据进行文本归一化处理，得到第三归一化数据；

对所述第三归一化数据进行加密，得到第四归一化数据；以及

将所述第四归一化数据在第三区块链网络中上链。

15．根据权利要求14所述的方法，还包括：

响应于来自第二客户端设备的数据调用请求，基于所述数据调用请求携带的调用类型信息，确定数据调用模型；

利用所述数据调用模型来处理所述第三区块链网络包括的第四区块链数据，得到第二目标区块链数据，其中，所述第四区块链数据包括所述第四归一化数据；以及

对所述第二目标区块链数据进行解密，并向所述第二客户端设备发送解密后的第二目标区块链数据。

16．一种区块链数据处理平台，包括：

区块链数据源管理模块，被配置为响应于接收到来自第一客户端设备的数据处理请求，基于所述数据处理请求携带的对象标识信息，从第一区块链网络中获取至少一个第一区块链数据；

私钥控制模块，被配置为基于所述数据处理请求携带的加密验证信息，对所述第一客户端设备进行确权；以及

数据处理模块，被配置为在确定所述第一客户端设备完成确权的情况下，向所述第一客户端设备发送所述至少一个第一区块链数据，以便所述第一客户端设备利用与所述至少一个第一区块链数据各自对应的区块体私钥，对所述至少一个第一区块链数据进行解密，得到至少一个第二区块链数据。

17．根据权利要求16所述的平台，其中，所述加密验证信息是由第一客户端设备

利用对象私钥对私钥摘要信息进行数字签名而得到的，所述私钥摘要信息是由第一客户端设备对与所述至少一个第一区块链数据各自对应的区块体私钥进行拼接和哈希计算而得到的；

其中，所述私钥控制模块被配置为：

基于所述对象标识信息，得到对象公钥，其中，所述对象公钥与所述对象私钥相对应；

利用所述对象公钥对所述加密验证信息进行验签，得到第一摘要信息，其中，在所述加密验证信息验签成功的情况下，所述第一摘要信息为所述私钥摘要信息；

向分布式私钥网络发送所述对象标识信息和所述第一摘要信息，以便所述分布式私钥网络根据所述对象标识信息，确定至少一个区块链体私钥，对所述至少一个区块体私钥进行拼接和哈希计算，得到第二摘要信息，并基于所述第一摘要信息和所述第二摘要信息的匹配结果，确定所述第一客户端设备的确权结果。

18．根据权利要求 16 所述的平台，其中，所述区块链数据源管理模块被配置为：

响应于所述数据处理请求，在未能从所述第一区块链网络中获取所述至少一个第一区块链数据的情况下，基于所述对象标识信息，分别对至少一个第二区块链网络进行跨链数据获取，得到所述至少一个第一区块链数据。

19．根据权利要求 18 所述的平台，其中，所述区块链数据源管理模块被配置为：

对于每个所述第二区块链网络，确定所述第二区块链网络的跨链节点；以及

基于所述跨链节点的节点类型，通过所述跨链节点来获取所述第一区块链数据。

20．根据权利要求 19 所述的平台，其中，所述区块链数据源管理模块被配置为：

在确定所述跨链节点为全节点的情况下，向所述跨链节点发送包括所述对象标识信息的数据获取请求，以便基于所述跨链节点返回的第一反馈数据，得到所述第一区块链数据；

其中，所述第一反馈数据是由所述跨链节点基于所述对象标识信息，从所述跨链节点的账本中得到的。

21．根据权利要求 19 所述的平台，其中，所述区块链数据源管理模块被配置为：

在确定所述跨链节点为轻节点的情况下，通过所述跨链节点向所述第二区块链网络的全节点发送包括所述对象标识信息的数据获取请求，以便基于所述全节点通过所述跨链节点返回的第二反馈数据，得到所述第一区块链数据；

其中，所述第二反馈数据是由所述全节点基于由所述跨链节点转发的所述对象标

识信息，从所述全节点的账本中得到的。

22．根据权利要求 18 所述的平台，其中，所述区块链数据源管理模块被配置为：

对于每个所述第二区块链网络，在所述第二区块链网络为公有链网络的情况下，向所述第二区块链网络包括的多个区块链节点广播包括所述对象标识信息的数据获取请求；以及

基于所述多个区块链节点各自返回的第三反馈数据，得到所述第一区块链数据，其中，所述第三反馈数据是由所述区块链节点基于所述对象标识信息，从所述区块链节点的账本中得到的。

23．根据权利要求 19 所述的平台，其中，所述加密验证信息是由第一客户端设备利用对象私钥对验证信息明文进行数字签名而得到的，所述验证信息明文是由所述第一客户端设备对加密组合信息进行哈希计算得到的；

其中，所述私钥控制模块被配置为：

基于所述对象标识信息，得到预留加密组合信息和对象公钥，其中，所述对象公钥与所述对象私钥相对应；

利用所述对象公钥对所述加密验证信息进行验签，得到第一验证信息，其中，在确定所述加密验证信息验签成功的情况下，所述第一验证信息为所述验证信息明文；

对所述预留加密组合信息进行哈希计算，得到第二验证信息；以及

基于所述第一验证信息和所述第二验证信息的匹配结果，确定所述第一客户端设备的确权结果。

24．根据权利要求 23 所述的平台，其中，所述加密组合信息或所述预留加密组合信息包括以下至少一项：

预设问题的答案文本，密码字符串，生物特征信息。

25．根据权利要求 16 所述的平台，所述私钥控制模块被配置为：

在确定所述第一客户端设备完成确权的情况下，向分布式私钥网络发送所述对象标识信息和至少一个所述第一区块链数据，以便所述分布式私钥网络根据所述对象标识信息，利用所述至少一个第二区块链网络各自的区块体私钥，对对应的至少一个所述第一区块链数据进行解密，得到至少一个第二区块链数据。

26．根据权利要求 25 所述的平台，其中，所述数据处理模块被配置为：

对于每个所述第二区块链网络，对所述第二区块链网络的第二区块链数据进行文本归一化处理，得到第一归一化数据；

利用与所述第二区块链网络对应的区块体公钥对所述第一归一化数据进行加密，得到第二归一化数据，其中，所述区块体公钥与所述区块体私钥相对应；

将所述第二归一化数据写入内存；以及

响应于检测到所述第一客户端设备通过预设接口访问所述内存，向所述第一客户端设备发送所述至少一个第二区块链网络各自的第二归一化数据，其中，所述第一客户端设备被配置为针对每个第二区块链网络，利用与所述第二区块链网络对应的区块体私钥对所述第二区块链网络的第二归一化数据进行解密，得到所述第一归一化数据，并将所述第一归一化数据渲染并展示在所述第一客户端设备的显示界面上。

27．根据权利要求 16~26 中任一项所述的平台，其中，所述数据处理模块被配置为：

在从所述至少一个第二区块链网络中跨链获取得到所述至少一个第一区块链数据的情况下，将所述至少一个第一区块链数据在所述第一区块链网络中上链。

28．根据权利要求 16~26 中任一项所述的平台，其中，所述数据处理模块被配置为：

将所述至少一个第一区块链数据写入内存；以及

响应于检测到所述第一客户端设备通过预设接口访问所述内存，向所述第一客户端设备发送所述至少一个第一区块链数据，其中，所述第一客户端设备被配置为利用与所述至少一个第一区块链数据各自对应的区块体私钥，对所述至少一个第一区块链数据进行解密，得到至少一个第二区块链数据，调用文本分类服务对所述至少一个第二区块链数据进行归一化处理，得到至少一个第一归一化数据，并将所述至少一个第一归一化数据渲染并展示在所述第一客户端设备的显示界面上。

29．根据权利要求 16~26 中任一项所述的平台，其中，所述数据处理模块被配置为：

响应于来自所述第一客户端设备的数据共享请求，获取所述数据共享请求携带的第一目标区块链数据；

对所述第一目标区块链数据进行文本归一化处理，得到第三归一化数据；

对所述第三归一化数据进行加密，得到第四归一化数据；以及

将所述第四归一化数据在第三区块链网络中上链。

30．根据权利要求 29 所述的平台，其中，所述数据处理模块被配置为：

响应于来自第二客户端设备的数据调用请求，基于所述数据调用请求携带的调用

类型信息，确定数据调用模型；

利用所述数据调用模型来处理所述第三区块链网络包括的第四区块链数据，得到第二目标区块链数据，其中，所述第四区块链数据包括所述第四归一化数据；以及

对所述第二目标区块链数据进行解密，并向所述第二客户端设备发送解密后的第二目标区块链数据。

31．一种区块链数据处理系统，包括：

第一客户端设备、第一区块链网络、区块链数据处理平台和分布式私钥网络；

其中，所述区块链数据处理平台被配置为：

响应于接收到来自第一客户端设备的数据处理请求，基于所述数据处理请求携带的对象标识信息，从第一区块链网络中获取至少一个第一区块链数据；

基于所述数据处理请求携带的加密验证信息，对所述第一客户端设备进行确权；

在确定所述第一客户端设备完成确权的情况下，向所述第一客户端设备发送所述至少一个第一区块链数据；

所述第一客户端设备被配置为：

利用与所述至少一个第一区块链数据各自对应的区块体私钥，对所述至少一个第一区块链数据进行解密，得到至少一个第二区块链数据。

32．根据权利要求31所述的系统，还包括：

至少一个第二区块链网络；

其中，所述区块链数据处理平台被配置为：

响应于所述数据处理请求，在未能从所述第一区块链网络中获取所述至少一个第一区块链数据的情况下，基于所述对象标识信息，分别对至少一个第二区块链网络进行跨链数据获取，得到所述至少一个第一区块链数据。

33．根据权利要求32所述的系统，其中，

所述区块链数据处理平台被配置为：

在确定所述第一客户端设备完成确权的情况下，向分布式私钥网络发送所述对象标识信息和至少一个所述第一区块链数据；

所述分布式私钥网络被配置为：

根据所述对象标识信息，利用所述至少一个第二区块链网络各自的区块体私钥，对对应的至少一个所述第一区块链数据进行解密，得到至少一个第二区块链数据。

34．根据权利要求33所述的系统，其中，所述分布式私钥网络被配置为：

响应于接收到来自区块链数据处理平台的对象标识信息和至少一个所述第一区块链数据，基于所述对象标识信息，从多个分布式节点中确定至少一个目标节点；

基于所述至少一个目标节点各自存储的私钥数据，得到所述至少一个第二区块链网络各自的区块体私钥；

利用所述至少一个第二区块链网络各自的区块体私钥，对对应的至少一个所述第一区块链数据进行解密，得到至少一个第二区块链数据；以及

向所述区块链数据处理平台发送所述至少一个第二区块链数据。

35．根据权利要求34所述的系统，其中，所述目标节点存储的私钥数据为字符串数据；

其中，所述分布式私钥网络被配置为：

对于每个所述目标节点，基于所述目标节点存储的私钥数据，得到拼接顺序信息和目标字符串数据；

基于所述至少一个目标节点各自的拼接顺序信息，将所述至少一个目标节点各自的目标字符串数据进行拼接，得到目标区块体私钥；以及

基于所述区块体私钥的预设字符长度，对所述目标区块体私钥进行切分，得到所述至少一个第二区块链网络各自的区块体私钥。

36．根据权利要求34所述的系统，其中，所述目标节点存储的私钥数据为曲线坐标数据；

其中，所述分布式私钥网络被配置为：

基于曲线模板，对所述至少一个目标节点各自存储的私钥数据进行曲线拟合，得到目标曲线；

将所述目标曲线包括的多个参数值进行拼接，得到目标区块体私钥；以及

基于所述区块体私钥的预设字符长度，对所述目标区块体私钥进行切分，得到所述至少一个第二区块链网络各自的区块体私钥。

37．一种区块链数据处理装置，包括：

第一获取模块，用于响应于接收到来自第一客户端设备的数据处理请求，基于所述数据处理请求携带的对象标识信息，从第一区块链网络中获取至少一个第一区块链数据；

确权模块，用于基于所述数据处理请求携带的加密验证信息，对所述第一客户端设备进行确权；以及

第一发送模块，用于在确定所述第一客户端设备完成确权的情况下，向所述第一客户端设备发送所述至少一个第一区块链数据，以便所述第一客户端设备利用与所述至少一个第一区块链数据各自对应的区块体私钥，对所述至少一个第一区块链数据进行解密，得到至少一个第二区块链数据。

38．一种电子设备，包括存储器和处理器，所述存储器中存储有所述处理器可执行的指令，所述指令在由所述处理器执行时使所述处理器执行如权利要求 1 至 15 中任一项所述的方法。

39．一种存储有计算机指令的非瞬时计算机可读存储介质，其中，所述计算机指令用于使所述计算机执行根据权利要求 1 至 15 中任一项所述的方法。

40．一种计算机程序产品，包括计算机程序，所述计算机程序在被处理器执行时实现根据权利要求 1 至 15 中任一项所述的方法。

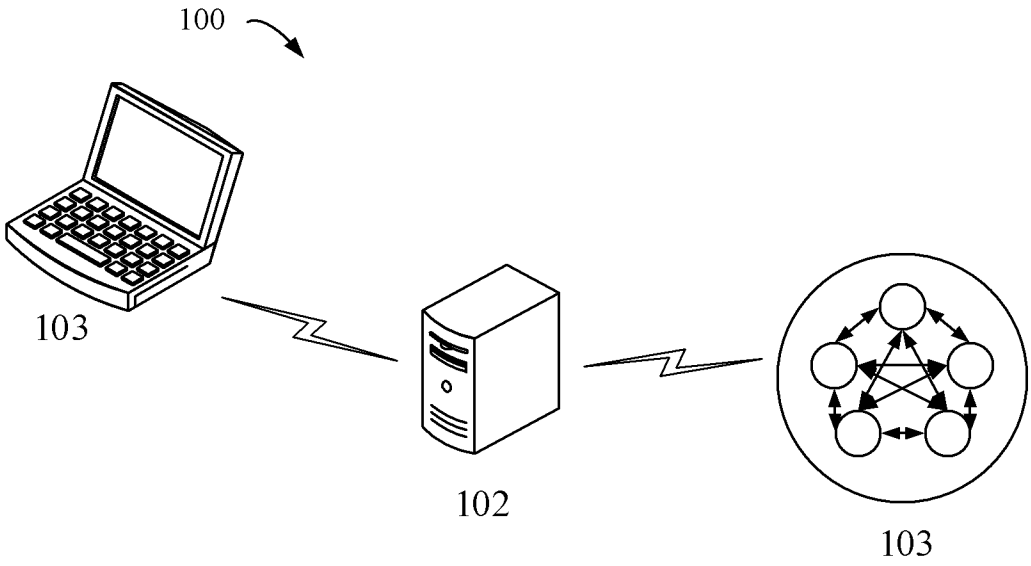
100
103
102
103

图 1

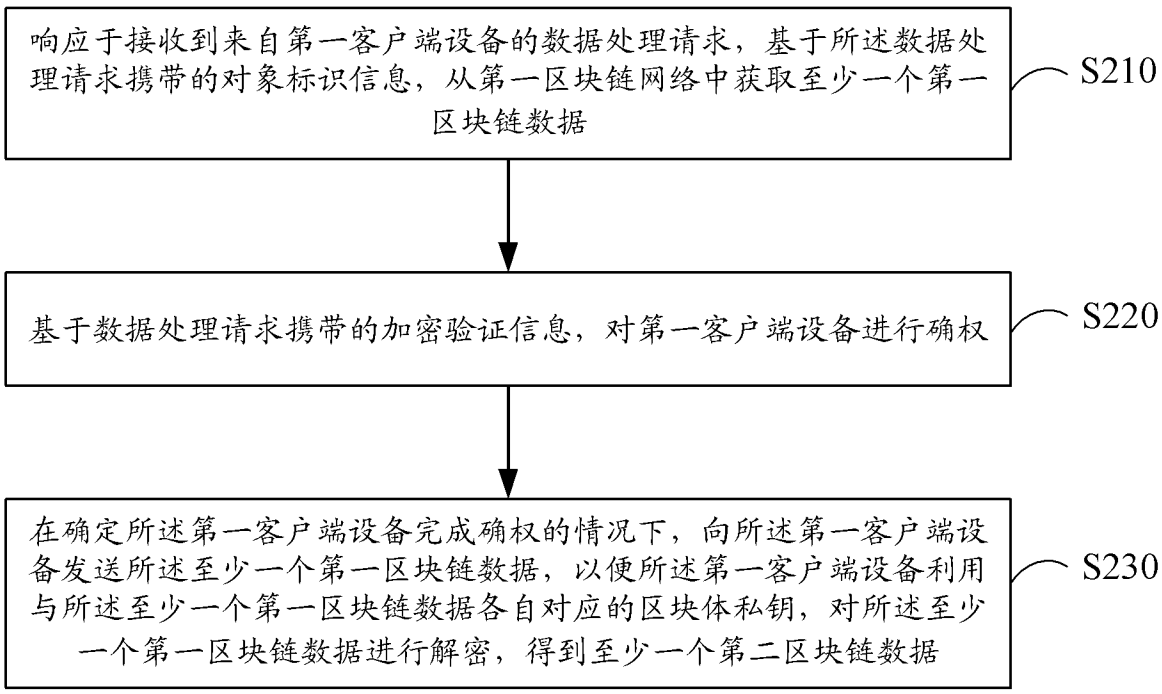
响应于接收到来自第一客户端设备的数据处理请求，基于所述数据处理请求携带的对象标识信息，从第一区块链网络中获取至少一个第一区块链数据
S210
基于数据处理请求携带的加密验证信息，对第一客户端设备进行确权
S220
在确定所述第一客户端设备完成确权的情况下，向所述第一客户端设备发送所述至少一个第一区块链数据，以便所述第一客户端设备利用与所述至少一个第一区块链数据各自对应的区块体私钥，对所述至少一个第一区块链数据进行解密，得到至少一个第二区块链数据
S230

图 2

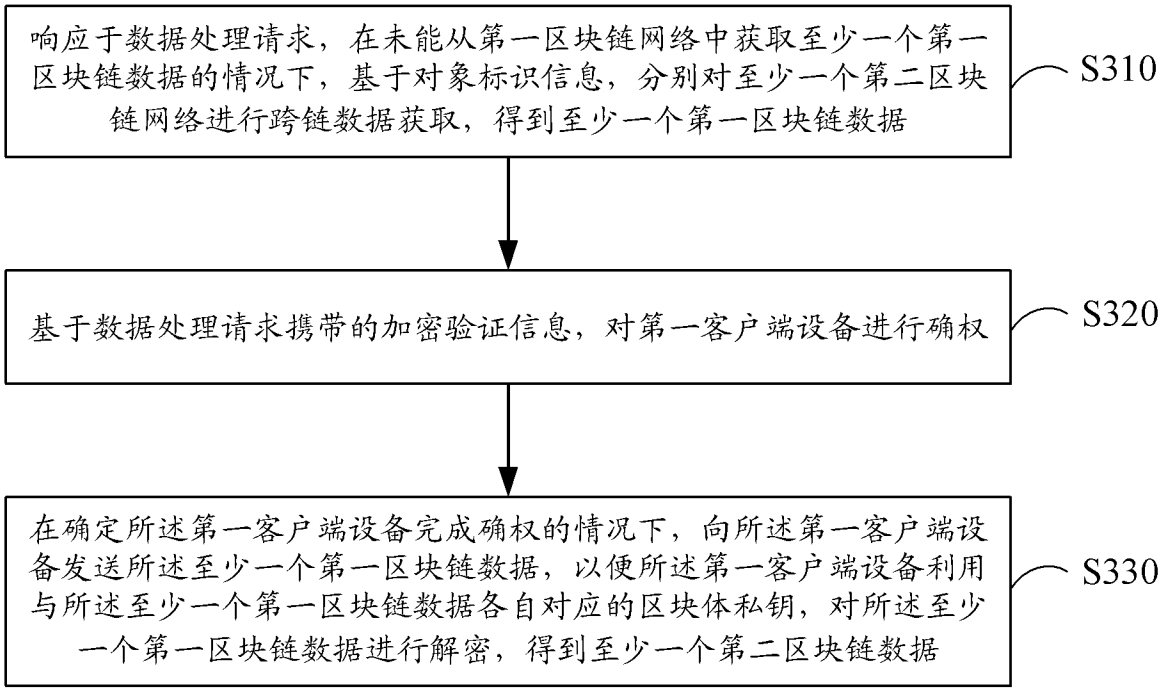
响应于数据处理请求，在未能从第一区块链网络中获取至少一个第一区块链数据的情况下，基于对象标识信息，分别对至少一个第二区块链网络进行跨链数据获取，得到至少一个第一区块链数据
S310
基于数据处理请求携带的加密验证信息，对第一客户端设备进行确权
S320
在确定所述第一客户端设备完成确权的情况下，向所述第一客户端设备发送所述至少一个第一区块链数据，以便所述第一客户端设备利用与所述至少一个第一区块链数据各自对应的区块体私钥，对所述至少一个第一区块链数据进行解密，得到至少一个第二区块链数据
S330

图 3

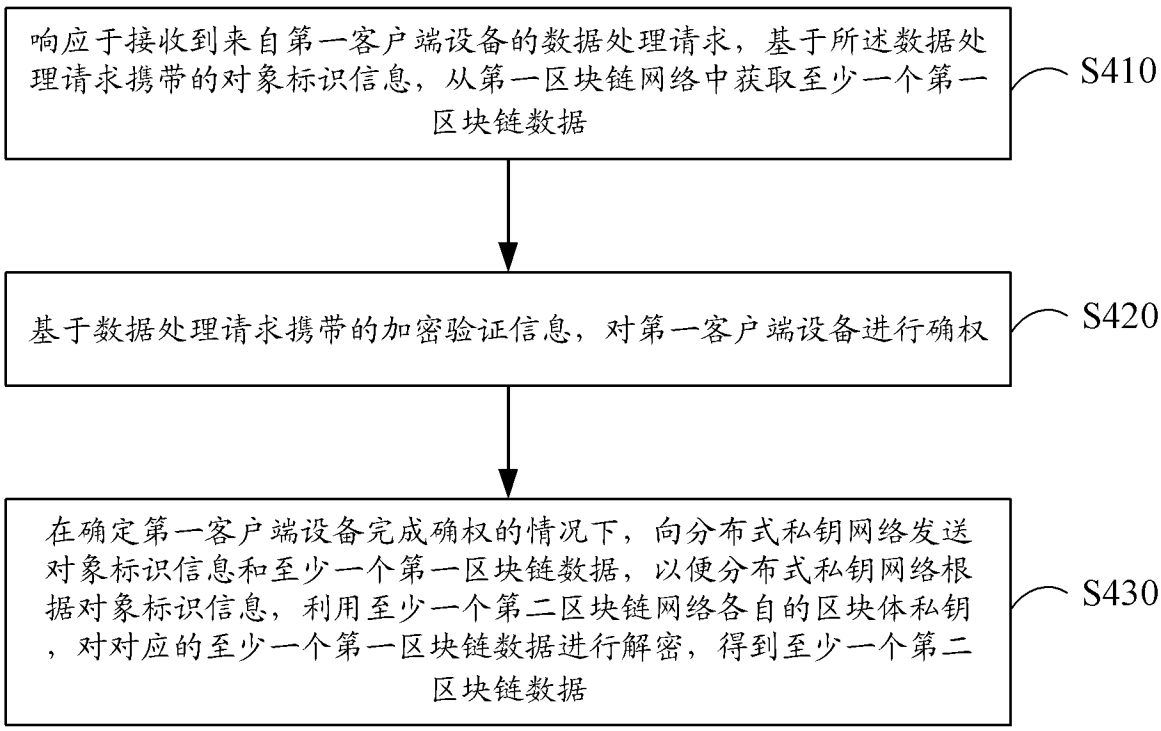
响应于接收到来自第一客户端设备的数据处理请求，基于所述数据处理请求携带的对象标识信息，从第一区块链网络中获取至少一个第一区块链数据
S410
基于数据处理请求携带的加密验证信息，对第一客户端设备进行确权
S420
在确定第一客户端设备完成确权的情况下，向分布式私钥网络发送对象标识信息和至少一个第一区块链数据，以便分布式私钥网络根据对象标识信息，利用至少一个第二区块链网络各自的区块体私钥，对对应的至少一个第一区块链数据进行解密，得到至少一个第二区块链数据
S430

图 4

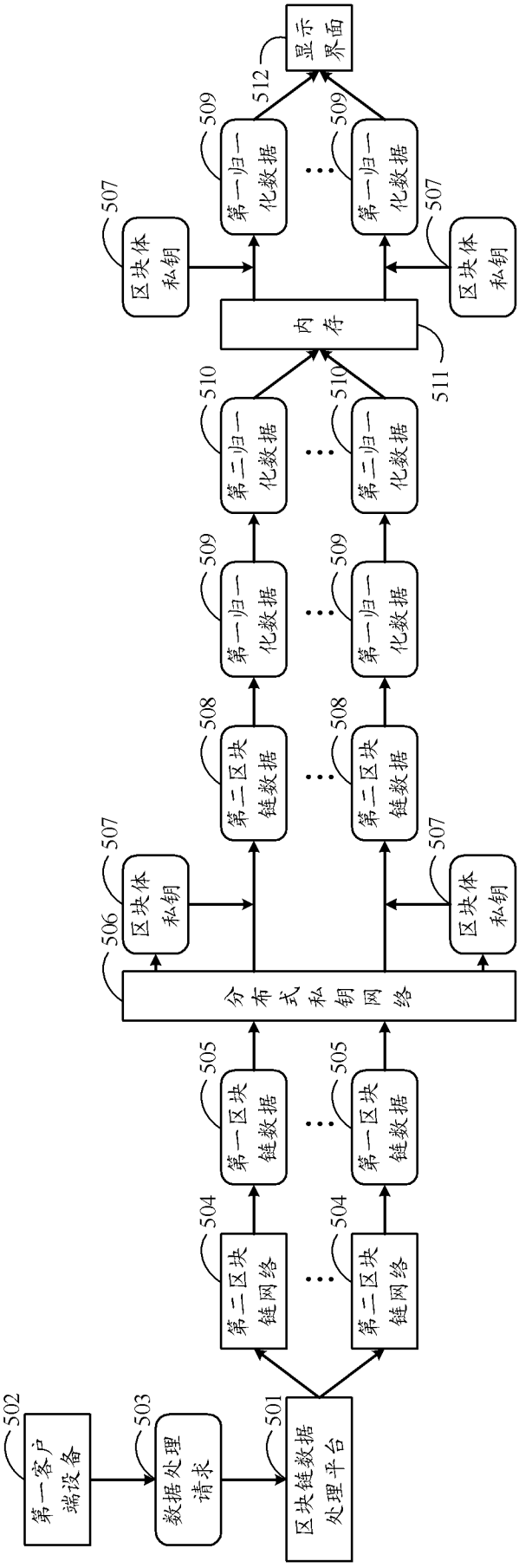
第一客户端设备
502
数据处理请求
503
区块链数据处理平台
501
第二区块链网络
504
第一区块链数据
505
分布式私钥网络
506
区块体私钥
507
第二区块链数据
508
第一归一化数据
509
第二归一化数据
510
内存
511
显示界面
512

图 5A

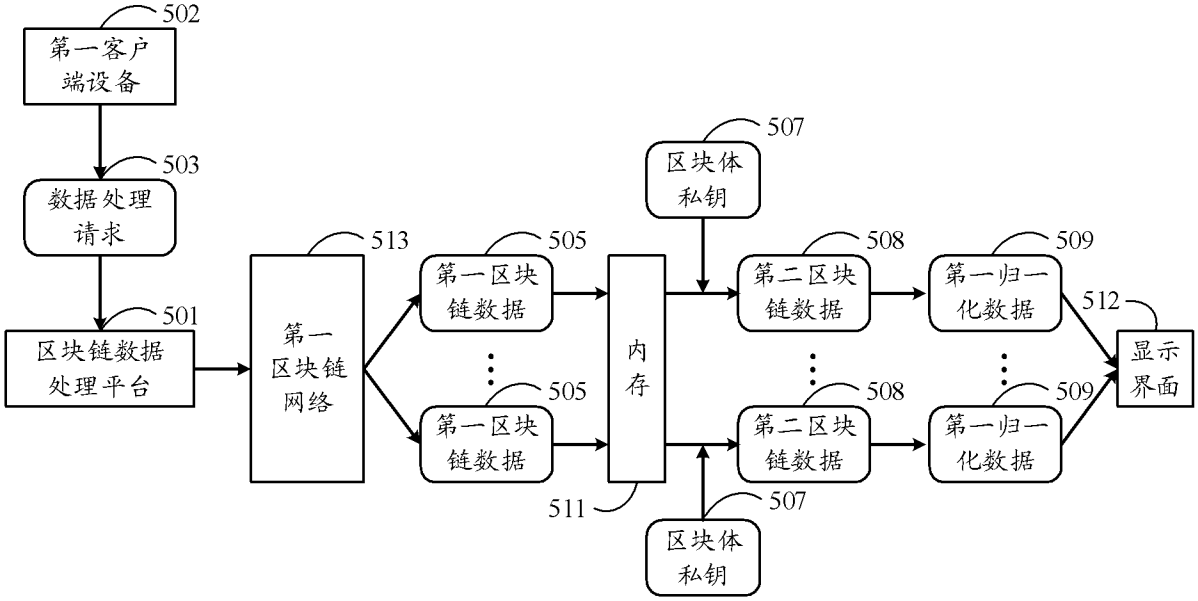
502
第一客户端设备
503
数据处理请求
501
区块链数据处理平台
513
第一区块链网络
505
第一区块链数据
505
第一区块链数据
507
区块体私钥
内存
511
507
区块体私钥
508
第二区块链数据
508
第二区块链数据
509
第一归一化数据
509
第一归一化数据
512
显示界面

图 5B

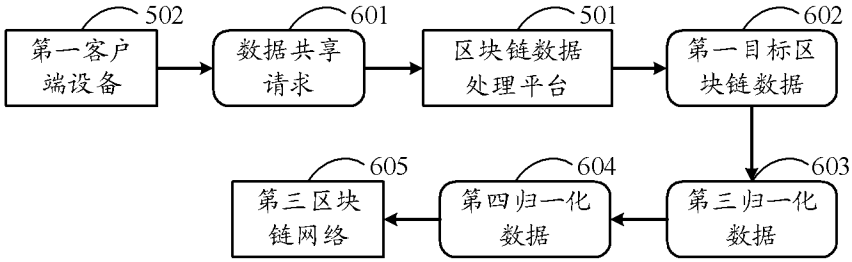
502
第一客户端设备
601
数据共享请求
501
区块链数据处理平台
602
第一目标区块链数据
603
第三归一化数据
604
第四归一化数据
605
第三区块链网络

图 6

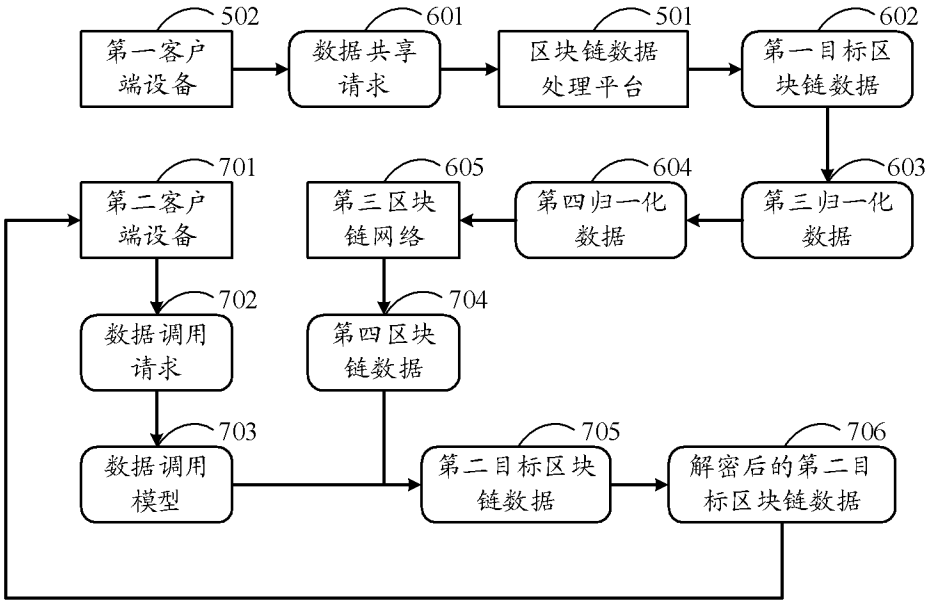
502
第一客户端设备
601
数据共享请求
501
区块链数据处理平台
602
第一目标区块链数据
603
第三归一化数据
604
第四归一化数据
605
第三区块链网络
701
第二客户端设备
702
数据调用请求
703
数据调用模型
704
第四区块链数据
705
第二目标区块链数据
706
解密后的第二目标区块链数据

图 7

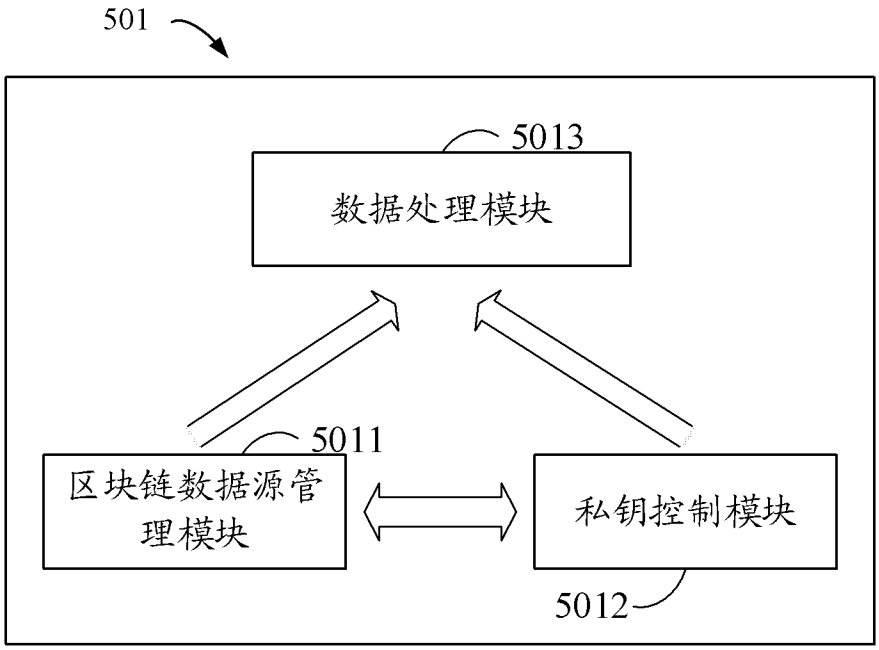
501
5013
数据处理模块
5011
区块链数据源管理模块
私钥控制模块
5012

图 8

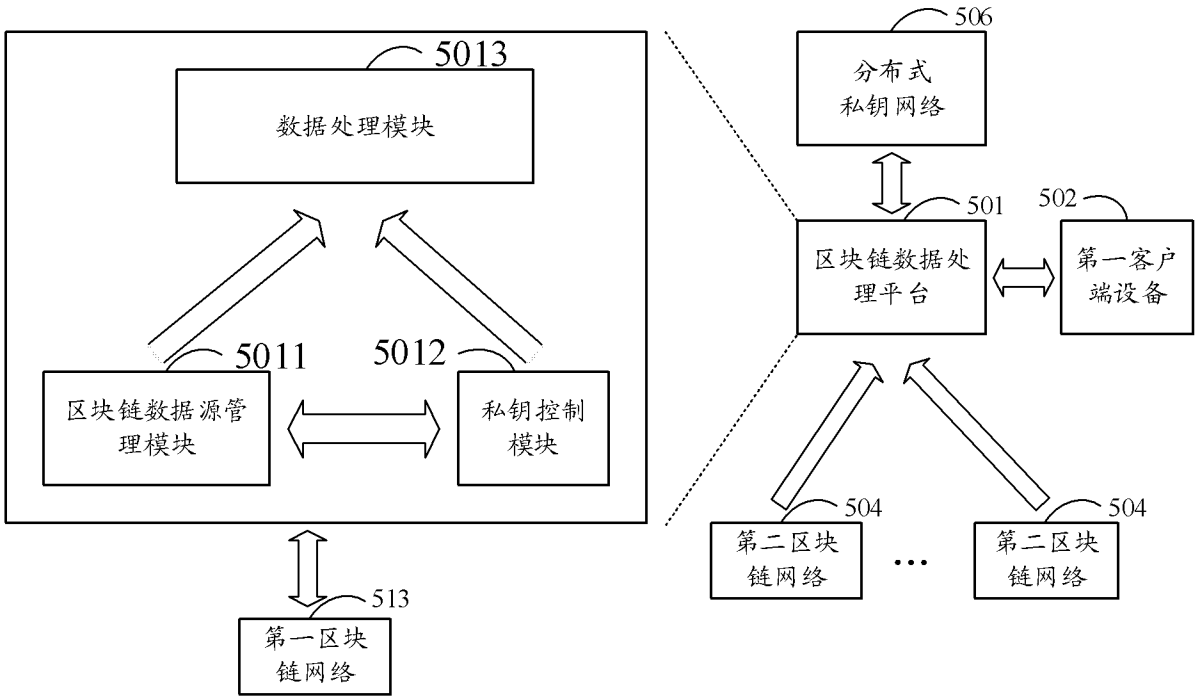
5013
数据处理模块
5011
5012
区块链数据源管理模块
私钥控制模块
513
第一区块链网络
506
分布式私钥网络
501
502
区块链数据处理平台
第一客户端设备
504
504
第二区块链网络
第二区块链网络

图 9

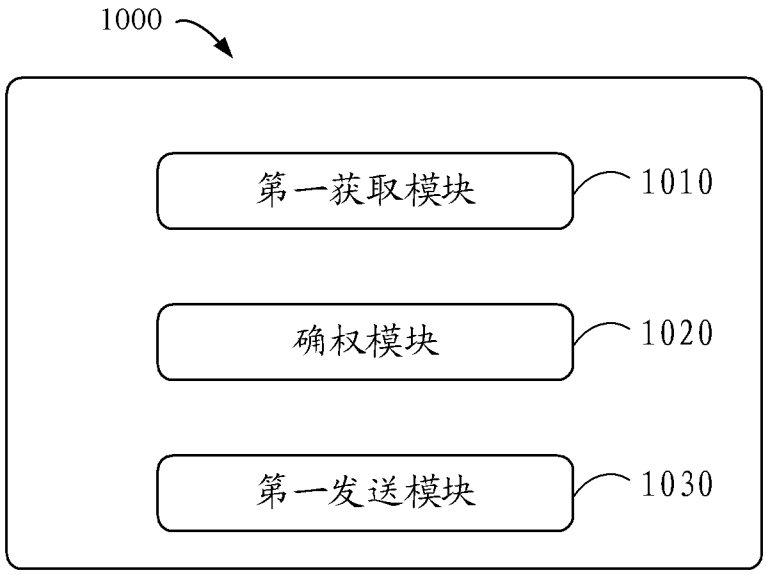
1000
第一获取模块
1010
确权模块
1020
第一发送模块
1030

图 10

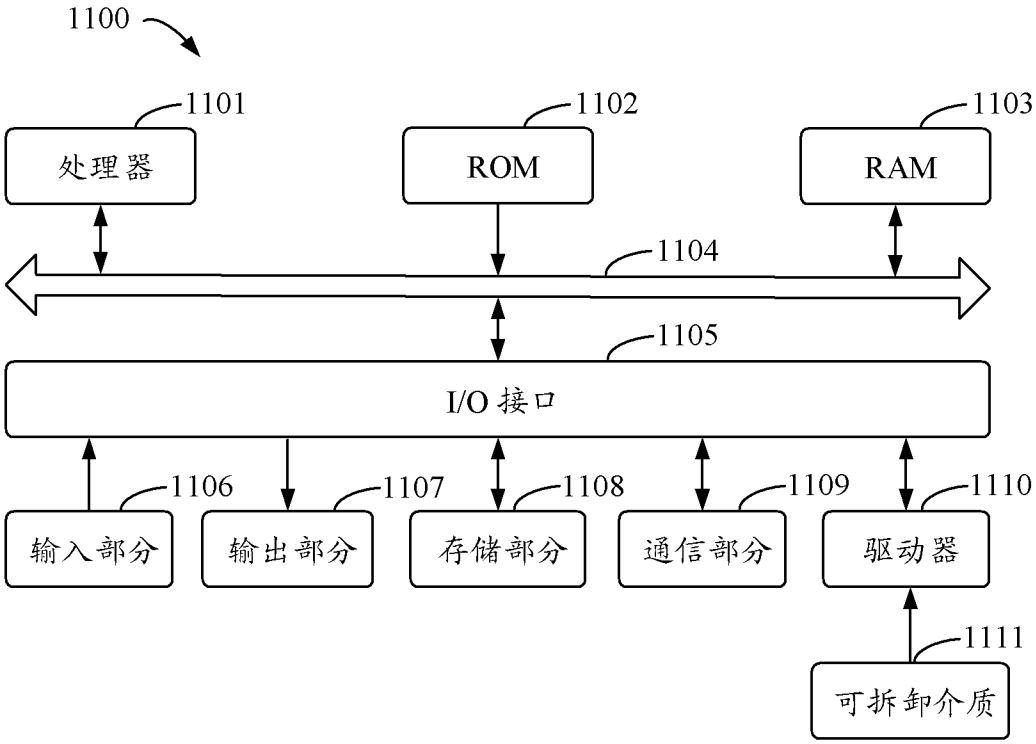
1100
1101
处理器
1102
ROM
1103
RAM
1104
1105
I/O 接口
1106
输入部分
1107
输出部分
1108
存储部分
1109
通信部分
1110
驱动器
1111
可拆卸介质

图 11

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2023/085649

A. CLASSIFICATION OF SUBJECT MATTER

G06F21/60(2013.01)i; H04L9/32(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)

IPC: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)

CNTXT, ENTXT, DWPI, CNKI: 客户端, 跨链, 密钥, 轻节点, 区块链, 全节点, 数据, 私钥, 摘要, client, cross, blockchain, key, light node, core node, digest, encrypt+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 113742782 A (CHINA ACADEMY OF INFORMATION AND COMMUNICATIONS TECHNOLOGY) 03 December 2021 (2021-12-03) description, paragraphs [0042]-[0126]	1-40
A	CN 114679274 A (ALIPAY (HANGZHOU) INFORMATION TECHNOLOGY LIMITED COMPANY et al.) 28 June 2022 (2022-06-28) entire document	1-40
A	WO 2022252941 A1 (TENCENT TECHNOLOGY (SHENZHEN) CO., LTD.) 08 December 2022 (2022-12-08) entire document	1-40
A	US 2021099311 A1 (DIVI LABS AND TECHNOLOGIES SOCIEDAD ANONIMA) 01 April 2021 (2021-04-01) entire document	1-40

☐ 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
"D" document cited by the applicant in the international application
"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
27 November 2023	**01 December 2023**

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

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2023/085649

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 113742782 A	03 December 2021	WO 2023077794 A1	11 May 2023
CN 114679274 A	28 June 2022	WO 2023124746 A1	06 July 2023
WO 2022252941 A1	08 December 2022	US 2023262126 A1	17 August 2023
		WO 2022252941 A1	08 December 2022
US 2021099311 A1	01 April 2021	None	

国际检索报告

国际申请号
PCT/CN2023/085649

A. 主题的分类

G06F21/60(2013.01)i；H04L9/32(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)

IPC: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））

CNTXT,ENTXT,DWPI,CNKI:客户端,跨链,密钥,轻节点,区块链,全节点,数据,私钥,摘要,client,cross,blockchain,key,light node,core node,digest,encrypt+

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
X	CN 113742782 A (中国信息通信研究院) 2021年12月3日 (2021 - 12 - 03) 说明书第[0042]-[0126]段	1-40
A	CN 114679274 A (支付宝（杭州）信息技术有限公司 等) 2022年6月28日 (2022 - 06 - 28) 全文	1-40
A	WO 2022252941 A1 (TENCENT TECHNOLOGY (SHENZHEN) COMPANY LIMITED) 2022年12月8日 (2022 - 12 - 08) 全文	1-40
A	US 2021099311 A1 (DIVI LABS AND TECHNOLOGIES SOCIEDAD ANONIMA) 2021年4月1日 (2021 - 04 - 01) 全文	1-40

☐ 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

“D” 申请人在国际申请中引证的文件

“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
2023年11月27日	2023年12月1日
ISA/CN的名称和邮寄地址 中国国家知识产权局 中国北京市海淀区蓟门桥西土城路6号 100088	受权官员 陈红英 电话号码 (+86) 010-53961636

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2023/085649

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	113742782	A	2021年12月3日	WO	2023077794	A1	2023年5月11日
CN	114679274	A	2022年6月28日	WO	2023124746	A1	2023年7月6日
WO	2022252941	A1	2022年12月8日	US	2023262126	A1	2023年8月17日
				WO	2022252941	A1	2022年12月8日
US	2021099311	A1	2021年4月1日		无		