

(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
2021 年 2 月 4 日 (04.02.2021)



(10) 国际公布号
WO 2021/017441 A1

(51) 国际专利分类号:
G06F 21/30 (2013.01)

(21) 国际申请号: PCT/CN2020/072153

(22) 国际申请日: 2020 年 1 月 15 日 (15.01.2020)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910703796.X 2019 年 7 月 31 日 (31.07.2019) CN

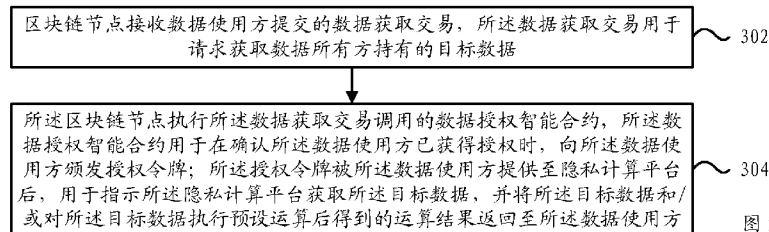
(71) 申请人: 创新先进技术有限公司 (ADVANCED NEW TECHNOLOGIES CO., LTD.) [—/CN]; 开曼群岛大开曼岛乔治镇医院路 27 号开曼企业中心, Grand Cayman KY1-9008 (KY)。

(72) 发明人: 魏长征 (WEI, Changzheng); 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。 闫莺 (YAN, Ying); 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。 张辉 (ZHANG, Hui); 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。 彭玉军 (PENG, Yujun); 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。

(74) 代理人: 北京博思佳知识产权代理有限公司 (BEIJING BESTIPR INTELLECTUAL PROPERTY LAW CORPORATION); 中国北京市

(54) Title: BLOCKCHAIN-BASED DATA AUTHORIZATION METHOD AND APPARATUS

(54) 发明名称: 基于区块链的数据授权方法及装置



302 A blockchain node receives a data acquisition transaction submitted by a data user, the data acquisition transaction being used for requesting to acquire target data held by a data owner

304 The blockchain node executes a data authorization smart contract called by the data acquisition transaction, the data authorization smart contract being used for issuing an authorization token to the data user when confirmed that the data user has been authorized, and the authorization token being used for instructing a privacy computing platform to acquire the target data after being provided to the privacy computing platform by the data user; and return to the data user the target data and/or an operation result obtained by executing a preset operation on the target data

(57) Abstract: Provided in one or more embodiment(s) of the present description are a blockchain-based data authorization method and apparatus. The method may comprise: a blockchain node receiving a data acquisition transaction submitted by a data user, the data acquisition transaction being used for requesting to acquire target data held by a data owner; the blockchain node executing a data authorization smart contract called by the data acquisition transaction, the data authorization smart contract being used for issuing an authorization token to the data user when confirmed that the data user has been authorized, and the authorization token being used for instructing a privacy computing platform to acquire the target data after being provided to the privacy computing platform by the data user; and returning to the data user the target data and/or an operation result obtained by executing a preset operation on the target data.

海淀区上地三街9号嘉华大厦B座409,
Beijing 100085 (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))。

(57) 摘要: 本说明书一个或多个实施例提供一种基于区块链的数据授权方法及装置, 该方法可以包括: 区块链节点接收数据使用方提交的数据获取交易, 所述数据获取交易用于请求获取数据所有方持有的目标数据; 所述区块链节点执行所述数据获取交易调用的数据授权智能合约, 所述数据授权智能合约用于在确认所述数据使用方已获得授权时, 向所述数据使用方颁发授权令牌; 所述授权令牌被所述数据使用方提供至隐私计算平台后, 用于指示所述隐私计算平台获取所述目标数据, 并将所述目标数据和/或对所述目标数据执行预设运算后得到的运算结果返回至所述数据使用方。

基于区块链的数据授权方法及装置

技术领域

[01] 本说明书一个或多个实施例涉及区块链技术领域，尤其涉及一种基于区块链的数据授权方法及装置。

5 背景技术

[02] 区块链技术（也被称之为，分布式账本技术）是一种去中心化的分布式数据库技术，具有去中心化、公开透明、不可篡改、可信任等多种特点，适用于诸多对数据可靠性具有高需求的应用场景中。

发明内容

10 [03] 有鉴于此，本说明书一个或多个实施例提供一种基于区块链的数据授权方法及装置。

[04] 为实现上述目的，本说明书一个或多个实施例提供技术方案如下：

[05] 根据本说明书一个或多个实施例的第一方面，提出了一种基于区块链的数据授权方法，包括：

15 [06] 区块链节点接收数据使用方提交的数据获取交易，所述数据获取交易用于请求获取数据所有方持有的目标数据；

[07] 所述区块链节点执行所述数据获取交易调用的数据授权智能合约，所述数据授权智能合约用于在确认所述数据使用方已获得授权时，向所述数据使用方颁发授权令牌；所述授权令牌被所述数据使用方提供至隐私计算平台后，用于指示所述隐私计算平台获取所述目标数据，并将所述目标数据和/或对所述目标数据执行预设运算后得到的运算结果返回至所述数据使用方。

20 [08] 根据本说明书一个或多个实施例的第二方面，提出了一种基于区块链的数据授权方法，包括：

[09] 隐私计算平台获取数据使用方提供的授权令牌，所述授权令牌由区块链上的数据授权智能合约向所述数据使用方颁发，表明所述数据使用方获得了对数据所有方持有的目标数据的授权；

25

[10] 所述隐私计算平台获取所述目标数据，以将所述目标数据和/或对所述目标数据执行预设运算后得到的运算结果返回至所述数据使用方。

[11] 根据本说明书一个或多个实施例的第三方面，提出了一种基于区块链的数据授权装置，包括：

5 [12] 接收单元，使区块链节点接收数据使用方提交的数据获取交易，所述数据获取交易用于请求获取数据所有方持有的目标数据；

[13] 执行单元，使所述区块链节点执行所述数据获取交易调用的数据授权智能合约，所述数据授权智能合约用于在确认所述数据使用方已获得授权时，向所述数据使用方颁发授权令牌；所述授权令牌被所述数据使用方提供至隐私计算平台后，用于指示所述隐私计算平台获取所述目标数据，并将所述目标数据和/或对所述目标数据执行预设运算后得到的运算结果返回至所述数据使用方。

10

[14] 根据本说明书一个或多个实施例的第四方面，提出了一种基于区块链的数据授权装置，包括：

[15] 令牌获取单元，使隐私计算平台获取数据使用方提供的授权令牌，所述授权令牌由区块链上的数据授权智能合约向所述数据使用方颁发，表明所述数据使用方获得了对数据所有方持有的目标数据的授权；

15

[16] 数据获取单元，使所述隐私计算平台获取所述目标数据，以将所述目标数据和/或对所述目标数据执行预设运算后得到的运算结果返回至所述数据使用方。

[17] 根据本说明书一个或多个实施例的第五方面，提出了一种电子设备，包括：

20 [18] 处理器；

[19] 用于存储处理器可执行指令的存储器；

[20] 其中，所述处理器通过运行所述可执行指令以实现如第一方面所述的方法。

[21] 根据本说明书一个或多个实施例的第六方面，提出了一种计算机可读存储介质，其上存储有计算机指令，该指令被处理器执行时实现如第一方面所述方法的步骤。

25 [22] 根据本说明书一个或多个实施例的第七方面，提出了一种电子设备，包括：

[23] 处理器；

[24] 用于存储处理器可执行指令的存储器；

[25] 其中，所述处理器通过运行所述可执行指令以实现如第二方面所述的方法。

[26] 根据本说明书一个或多个实施例的第八方面，提出了一种计算机可读存储介质，其上存储有计算机指令，该指令被处理器执行时实现如第二方面所述方法的步骤。

附图说明

5 [27] 图 1 是一示例性实施例提供的一种示例环境的示意图。

[28] 图 2 是一示例性实施例提供的一种概念架构的示意图。

[29] 图 3 是一示例性实施例提供的一种基于区块链的数据授权方法的流程图。

[30] 图 4 是一示例性实施例提供的另一种基于区块链的数据授权方法的流程图。

10 [31] 图 5 是一示例性实施例提供的一种基于区块链网络实现的端到端数据授权的示意图。

[32] 图 6 是一示例性实施例提供的一种基于区块链网络实现的端到端数据授权的交互流程图。

[33] 图 7 是一示例性实施例提供的一种授权令牌的示意图。

15 [34] 图 8 是一示例性实施例提供的另一种基于区块链网络实现的端到端数据授权的示意图。

[35] 图 9 是一示例性实施例提供的一种设备的结构示意图。

[36] 图 10 是一示例性实施例提供的一种基于区块链的数据授权装置的框图。

[37] 图 11 是一示例性实施例提供的另一种设备的结构示意图。

[38] 图 12 是一示例性实施例提供的另一种基于区块链的数据授权装置的框图。

20 具体实施方式

[39] 这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所述实施方式并不代表与本说明书一个或多个实施例相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本说明书一个或多个实施例的一些方面相一致的装置和方法的例子。

25

[40] 需要说明的是：在其他实施例中并不一定按照本说明书示出和描述的顺序来执行相应方法的步骤。在一些其他实施例中，其方法所包括的步骤可以比本说明书所描述的更多或更少。此外，本说明书中所描述的单个步骤，在其他实施例中可能被分解为多个步骤进行描述；而本说明书中所描述的多个步骤，在其他实施例中也可能被合并为单个步骤进行描述。

[41] 图 1 是一示例性实施例提供的一种示例环境的示意图。如图 1 所示，示例环境 100 允许实体参与区块链网络 102。区块链网络 102 可以为公有类型、私有类型或联盟类型的区块链网络。示例环境 100 可以包括计算设备 104、106、108、110、112 和网络 114；在一实施例中，网络 114 可以包括局域网（Local Area Network, LAN）、广域网（Wide Area Network, WAN）、因特网或其组合，并连接至网站、用户设备（例如计算设备）和后端系统。在一实施例中，可以通过有线和/或无线通信方式访问网络 114。

[42] 在某些情况下，计算设备 106、108 可以是云计算系统的节点（未显示），或者每个计算设备 106、108 可以是单独的云计算系统，包括由网络互连并作为分布式处理系统工作的多台计算机。

[43] 在一实施例中，计算设备 104~108 可以运行任何适当的计算系统，使其能够作为区块链网络 102 中的节点；例如，计算设备 104~108 可以包括但不限于服务器、台式计算机、笔记本电脑、平板电脑计算设备和智能手机。在一实施例中，计算设备 104~108 可以归属于相关实体并用于实现相应的服务，例如该服务可以用于对某一实体或多个实体之间的交易进行管理。

[44] 在一实施例中，计算设备 104~108 分别存储有区块链网络 102 对应的区块链账本。计算设备 104 可以是（或包含）用于提供浏览器功能的网络服务器，该网络服务器可基于网络 114 提供与区块链网络 102 相关的可视化信息。在一些情况下，计算设备 104 可以不参与区块验证，而是监控区块链网络 102 以确定其他节点（譬如可以包括计算设备 106-108）何时达成共识，并据此生成相应的区块链可视化用户界面。

[45] 在一实施例中，计算设备 104 可接收客户端设备（例如计算设备 110 或计算设备 112）针对区块链可视化用户界面发起的请求。在一些情况下，区块链网络 102 的节点也可以作为客户端设备，比如计算设备 108 的用户可以使用运行在计算设备 108 上的浏览器向计算设备 104 发送上述请求。

[46] 响应于上述请求，计算设备 104 可以基于存储的区块链账本生成区块链可视化用

户界面（如网页），并将生成的区块链可视化用户界面发送给请求的客户端设备。如果区块链网络 102 是私有类型或联盟类型的区块链网络，对区块链可视化用户界面的请求可以包括用户授权信息，在生成区块链可视化用户界面并发送给请求的客户端设备之前，可以由计算设备 104 对该用户授权信息进行验证，并在验证通过后返回相应的区块链可视化用户界面。

[47] 区块链可视化用户界面可以显示在客户端设备上（例如可显示在图 1 所示的用户界面 116 中）。当区块链账本发生更新时，用户界面 116 的显示内容也可以随之发生更新。此外，用户与用户界面 116 的交互可能导致对其他用户界面的请求，例如显示区块列表、区块详情、交易列表、交易详情、账户列表、账户详情、合约列表、合约详情或者用户对区块链网络实施搜索而产生的搜索结果页面等。

[48] 图 2 是一示例性实施例提供的一种概念架构的示意图。如图 2 所示，该概念架构 200 包括实体层 202、托管服务层 204 和区块链网络层 206。例如，实体层 202 可以包括三个实体：实体 1、实体 2 和实体 3，每个实体都有各自的交易管理系统 208。

[49] 在一实施例中，托管服务层 204 可以包括每个事务管理系统 208 对应的接口 210。例如，各个事务管理系统 208 使用协议（例如超文本传输协议安全（HTTPS）等）通过网络（例如图 1 中的网络 114）与各自的接口 210 通信。在一些例子中，每个接口 210 可以提供各自对应的交易管理系统 208 与区块链网络层 206 之间的通信连接；更具体地，接口 210 可与区块链网络层 206 的区块链网络 212 通信。在一些例子中，接口 210 和区块链网络层 206 之间的通信可以使用远程过程调用（Remote Procedure Calls, RPCs）而实现。在一些例子中，接口 210 可以向交易管理系统 208 提供用于访问区块链网络 212 的 API 接口。

[50] 如本文所述，区块链网络 212 以对等网络的形式提供，该对等网络包括多个节点 214，这些节点 214 分别用于对区块链数据所形成的区块链账本 216 进行持久化；其中，图 2 中仅示出了一份区块链账本 216，但区块链网络 212 中可以存在多份区块链账本 216 或其副本，比如每一节点 214 可以分别维护一份区块链账本 216 或其副本。

[51] 需要指出的是：在本说明书中所描述的交易（transaction），是指用户通过区块链的客户端创建，并需要最终发布至区块链的分布式数据库中的一笔数据。其中，区块链中的交易，存在狭义的交易以及广义的交易之分。狭义的交易是指用户向区块链发布的一笔价值转移；例如，在传统的比特币区块链网络中，交易可以是用户在区块链中发起的一笔转账。而广义的交易是指用户向区块链发布的一笔具有业务意图的业务数据；例

如，运营方可以基于实际的业务需求搭建一个联盟链，依托于联盟链部署一些与价值转移无关的其它类型的在线业务（比如，租房业务、车辆调度业务、保险理赔业务、信用服务、医疗服务等），而在这类联盟链中，交易可以是用户在联盟链中发布的一笔具有业务意图的业务消息或者业务请求。

5 [52] 区块链一般被划分为三种类型：公有链（Public Blockchain），私有链（Private Blockchain）和联盟链（Consortium Blockchain）。此外，还有多种类型的结合，比如私有链+联盟链、联盟链+公有链等不同组合形式。其中去中心化程度最高的是公有链。公有链以比特币、以太坊为代表，加入公有链的参与者可以读取链上的数据记录、参与交易以及竞争新区块的记账权等。而且，各参与者（即节点）可自由加入以及退出网络，
10 并进行相关操作。私有链则相反，该网络的写入权限由某个组织或者机构控制，数据读取权限受组织规定。简单来说，私有链可以为一个弱中心化系统，参与节点具有严格限制且少。这种类型的区块链更适合于特定机构内部使用。联盟链则是介于公有链以及私有链之间的区块链，可实现“部分去中心化”。联盟链中各个节点通常有与之相对应的实体机构或者组织；参与者通过授权加入网络并组成利益相关联盟，共同维护区块链运行。
15 行。

[53] 不论是公有链、私有链或是联盟链，本说明书均可以通过在区块链网络与链下的隐私计算平台之间实现协同，从而在数据所有方与数据使用方之间实现安全的端到端数据授权。下面结合实施例对本说明书的技术方案进行描述。

[54] 图 3 是一示例性实施例提供的一种基于区块链的数据授权方法的流程图。如图 3
20 所示，该方法应用于区块链节点，可以包括以下步骤：

[55] 步骤 302，区块链节点接收数据使用方提交的数据获取交易，所述数据获取交易用于请求获取数据所有方持有的目标数据。

[56] 数据使用方可以直接在上述区块链节点上生成数据获取交易；或者，数据使用方可以在客户端上生成数据获取交易，并通过客户端将该数据获取交易发送至上述区块链
25 节点；或者，数据使用方可以在客户端上生成数据获取交易后，将该数据获取交易发送至另一区块链节点，并由该另一区块链节点将该数据获取交易发送至上述区块链节点。当然，在上述数据获取交易通过共识后，该数据获取交易会被传输至区块链网络中的所有区块链节点，并分别由各个区块链节点执行该数据获取交易。

[57] 一般的，采用工作量证明（Proof of Work, POW）以及股权证明（Proof of Stake,

POS)、委任权益证明(Delegated Proof of Stake, DPOS)等共识算法的区块链网络中, 争夺记账权的节点都可以在接收到区块链交易后执行该区块链交易。争夺记账权的节点中可能其中一个在本轮争夺记账权的过程中胜出, 成为记账节点。以上述的数据获取交易为例, 记账节点可以将该数据获取交易与其它交易一起打包并生成新的区块, 并将生成的新的区块发送至其它节点进行共识。

[58] 对于采用实用拜占庭容错(Practical Byzantine Fault Tolerance, PBFT)等机制的区块链网络中, 具有记账权的节点在本轮记账前已经商定好。因此, 上述区块链节点接收到数据获取交易后, 如果自身不是本轮的记账节点, 则可以将该数据获取交易发送至记账节点。对于本轮的记账节点(可以是上述的区块链节点), 在将该数据获取交易打包并生成新区块的过程中或者之前, 或在将该数据获取交易与其它交易一起打包并生成新区块的过程中或者之前, 可以执行该数据获取交易。所述记账节点将该数据获取交易打包(或还包括其它交易一起打包)并生成新的区块后, 将生成的新的区块或者区块头发送至其它节点进行共识。

[59] 如上所述, 采用 POW 机制的区块链网络中, 或者采用 POS、DPOS、PBFT 机制的区块链网络中, 本轮的记账节点都可以将数据获取交易打包并生成新的区块, 并将生成的新的区块后区块头发送至其它节点进行共识。如果其它节点接收到所述区块后经验证没有问题, 可以将该新的区块追加到原有的区块链末尾, 从而完成记账过程, 达成共识; 其中, 若数据获取交易用于调用数据授权智能合约, 则完成了对该数据授权智能合约的调用和执行。其它节点验证记账节点发来的新的区块或区块头的过程中, 也可以执行所述区块中的数据获取交易。

[60] 步骤 304, 所述区块链节点执行所述数据获取交易调用的数据授权智能合约, 所述数据授权智能合约用于在确认所述数据使用方已获得授权时, 向所述数据使用方颁发授权令牌; 所述授权令牌被所述数据使用方提供至隐私计算平台后, 用于指示所述隐私计算平台获取所述目标数据, 并将所述目标数据和/或对所述目标数据执行预设运算后得到运算结果返回至所述数据使用方。

[61] 不论是公有链、私有链或是联盟链, 都可能提供智能合约的功能。区块链上的智能合约是在区块链系统上可以被交易触发执行的合约。智能合约可以通过代码的形式定义。以以太坊为例, 支持用户在以太坊网络中创建并调用一些复杂的逻辑, 这是以太坊区别于比特币区块链技术的最大挑战。以太坊作为一个可编程区块链的核心是以太坊虚拟机(EVM), 每个以太坊节点都可以运行 EVM。EVM 是一个图灵完备的虚拟机, 这

意味着可以通过它实现各种复杂的逻辑。用户在以太坊中发布和调用智能合约就是在EVM上运行的。

[62] 数据授权智能合约被创建后，在区块链上形成相应的合约账户，该合约账户存在特定的合约地址。数据获取交易可以在诸如该数据获取交易的to字段包含上述的合约地址，以调用数据授权智能合约。如前所述，区块链网络中的所有区块链节点之间完成共识后，每个区块链节点分别接收到数据获取交易、读取该数据获取交易的to字段并调用上述的数据授权智能合约，具体是指将数据授权智能合约的代码读入区块链节点上的EVM中予以执行。

[63] 数据授权智能合约可以包含对应的授权方名单，以用于记录对数据所有方持有的数据已获得授权的对象信息，即授权方的信息。那么，如果数据授权智能合约确认数据使用方位于授权方名单内，则可以确认该数据使用方已获得授权。基于授权方名单的管理方式，可以对数据所有方所持有的全部数据进行一次授权，并且即便数据所有方所持有的数据发生增加或减少时，也不会影响授权方名单的内容，即能够兼容数据所有方所持有数据的更新。

[64] 在数据授权智能合约被创建时，授权方名单的信息可以被写入合约代码中，使得该授权方名单的内容不可更改。那么，可能需要对数据授权智能合约进行替换或版本迭代，以实现授权方名单的更新。或者，数据授权智能合约可以存在对应的一个或多个状态，区块链节点上可以维护该一个或多个状态的取值，当状态的取值为授权方的信息时，该一个或多个状态相当于上述的授权方名单；其中，数据所有方可以通过向区块链网络中提交区块链交易，该区块链交易可以调用数据授权智能合约中定义的授权接口，使得授权方名单的内容可以在数据授权智能合约被执行后发生更新，而无需对数据授权智能合约进行替换或版本迭代。或者，数据授权智能合约可以调用另一智能合约，该另一智能合约的代码或状态可以用于记录授权方名单；其中，如果授权方名单被不可更改地写入该另一智能合约的代码中，那么在需要对授权方名单进行更新时，可以创建新的智能合约、该新的智能合约的代码中包含更新后的授权方名单，然后由数据授权智能合约调用新的智能合约的合约地址即可（被调用的合约地址可以作为数据授权智能合约的一个状态，该状态的取值可以发生变化）；而如果授权方名单被写入上述另一智能合约对应的状态中，那么如前所述只需要对状态的取值进行更新，即可实现授权方名单的更新，而数据授权智能合约所调用的合约地址也无需更新，该合约地址既可以固定写入数据授权智能合约的代码中，也可以写入数据授权智能合约的一个状态中。

[65] 数据使用方可以临时向数据所有方请求获取授权。例如，数据使用方可以向区块链网络中提交授权请求交易，该授权请求交易调用上述数据授权智能合约中定义的请求接口，使得区块链节点执行该授权请求交易后，可以通过调用数据授权智能合约中定义的请求接口，使数据授权智能合约在交易日志中写入授权请求事件。然后，数据所有方可以通过事件监听回调机制，在监听到交易日志中写入的上述授权请求事件时做出响应。例如，当确定数据使用方能够获得授权时，数据所有方可以向区块链网络提交授权确认交易，该授权确认交易调用上述数据授权智能合约中定义的授权接口，使得区块链节点执行该授权确认交易后，可以通过调用数据授权智能合约中定义的授权接口，使数据授权智能合约将数据使用方标记为已获得授权。将数据使用方标记为已获得授权，一种情况下可以是将数据使用方添加至授权方名单中，其添加过程如前文所述、此处不再赘述，那么只要数据使用方处于授权方名单内，即可随时请求获取数据所有方持有的数据，相当于数据使用方获得了长期授权；另一种情况下，数据授权智能合约只是确认数据使用方的本次操作获得了授权，使得数据授权智能合约在完成授权令牌的颁发操作后，即可取消数据使用方的已授权状态，使数据使用方下次需要重新向数据所有方请求授权，才能够再次获得授权令牌。

[66] 虽然相比于上述的后一种情况而言，授权方名单属于一种长期授权，但是并不一定意味着永久授权。例如，数据所有方可以通过更新授权方名单，将一个或多个授权方剔除、使其失去授权；再例如，授权方名单中的每一授权方可以存在一定数值的剩余授权时长和/或剩余授权次数，譬如数据授权智能合约可以在完成授权令牌的颁发操作后，递减数据使用方对应的剩余授权时长和/或剩余授权次数，那么当剩余授权时长或剩余授权次数清零时，相应的授权方可以被自动从授权方名单中剔除，相当于对授权方名单内的授权方实施的“老化”机制。

[67] 数据使用方可以在授权请求交易中包含目标数据的信息，该目标数据的信息可以被写入交易日志中的授权请求事件内，以使得数据所有方获知数据使用方所希望请求的授权范围；如果授权请求交易中并未包含任何数据的信息，则表明数据使用方请求获取数据所有方持有的全部数据的授权。相应地，数据所有方可以在授权确认交易中添加目标数据的信息，以表明针对该目标数据向数据使用方赋予授权；如果数据所有方提交的授权确认交易中并未包含任何数据的信息，则表明数据所有方向数据使用方开放了所有数据的授权。因此，在一些情况下，数据使用方的数据获取交易中包含的目标数据的信息可能与其所获得的授权范围（即获得了针对哪些数据的授权）不一致，此时可能导致最终无法成功获得目标数据。

[68] 数据获取交易中可以包含目标数据的描述信息，比如该目标数据的哈希值或其他任意描述信息，只要能够指向目标数据即可。例如，该目标数据的描述信息可以包含于数据获取交易的 data 字段中；当数据获取交易调用数据授权智能合约时，data 字段中的内容可以作为该数据授权智能合约的输入信息。相应地，数据授权智能合约在生成授权令牌时，可以在授权令牌中包含目标数据的描述信息，使得授权令牌仅用于获得该描述信息对应的上述目标数据，而非其他数据。当然，数据获取交易中可以不包含目标数据的描述信息，而仅包含数据所有方的信息，使得相应生成的授权令牌可以用于获得数据所有方的任意数据，这可由数据使用方后续向隐私计算平台提供授权令牌时，一并告知其希望获得的目标数据的描述信息。

[69] 数据使用方通过将授权令牌提供至隐私计算平台，使得隐私计算平台无需关注于数据使用方的身份、只需要识别该授权令牌，从而根据授权令牌获取目标数据。

[70] 目标数据可以存证于区块链上，譬如存储于区块链节点维护的数据库中。为了避免泄露目标数据，通常需要对目标数据进行加密后存储。例如，数据所有方可以向区块链网络中提交存证交易，该存证交易中包含加密后目标数据，使得区块链节点在收到存证交易后，可以对该存证交易中包含的加密后目标数据进行存储，其中加密后目标数据由数据所有方的公钥对目标数据进行加密后得到；相应地，数据所有方的私钥可以被托管于隐私计算平台处，使得隐私计算平台可以从区块链节点维护的数据库中读取加密后目标数据，并基于托管的数据所有方的私钥实施解密，以解密得到上述的目标数据。再例如，数据所有方可以向区块链网络中提交隐私存证交易，该隐私存证交易的交易内容处于加密状态（可采用对称加密、非对称加密或数字信封加密等方式实现）且该交易内容包含目标数据，使得区块链节点可以在可信执行环境中解密得到该隐私存证交易的交易内容、得到目标数据，并采用数据所有方的公钥在可信执行环境中对目标数据进行加密，得到加密后目标数据，以存储于区块链节点对应的数据库中；相应地，数据所有方的私钥可以被托管于隐私计算平台处，以使隐私计算平台获得加密后目标数据后，可以通过该私钥解密得到上述的目标数据。又例如，目标数据可以由区块链节点在可信执行环境中执行某一区块链交易（比如数据所有方提交的存证交易）的过程中生成，而区块链节点可以采用数据所有方的公钥在可信执行环境中对生成的目标数据进行加密，得到加密后目标数据，以存储于区块链节点对应的数据库中；相应地，数据所有方的私钥可以被托管于隐私计算平台处，以使隐私计算平台获得加密后目标数据后，可以通过该私钥解密得到上述的目标数据。

[71] 如前所述, 对于目标数据的加密处理, 可以结合可信执行环境 (Trusted Execution Environment, TEE) 来实现; 由于目标数据可以为数据使用方所请求、数据所有方持有的任意数据, 即数据所有方持有的任意数据均可以采用类似的方式实现加密处理。TEE 是基于 CPU 硬件的安全扩展, 且与外部完全隔离的可信执行环境。TEE 最早是由 Global Platform 提出的概念, 用于解决移动设备上资源的安全隔离, 平行于操作系统为应用程序提供可信安全的执行环境。例如, 英特尔的软件保护扩展 (SGX) 等 TEE 技术隔离了代码执行、远程证明、安全配置、数据的安全存储以及用于执行代码的可信路径。在 TEE 中运行的应用程序受到安全保护, 几乎不可能被第三方访问。

[72] 以 Intel SGX 技术为例。区块链节点利用 CPU 中新增的处理器指令, 在内存中可以分配一部分区域 EPC (Enclave Page Cache, 围圈页面缓存或飞地页面缓存), 将 EVM 加载至 EPC 中, 并通过远程证明确认所加载 EVM 的代码与密钥管理服务器处 EVM 的代码一致 (例如比较 hash 值)。在远程证明通过后, 区块链节点通过 CPU 内的加密引擎 MEE (Memory Encryption Engine) 对上述目标数据进行加密存入所述 EPC 中。EPC 中加密的内容只有进入 CPU 后才能够被解密成明文。在 CPU 中, 对明文的目标数据进行加密, 得到加密后目标数据, 以存储于区块链节点对应的数据库中; 类似地, 区块链节点可以在 TEE 中对加密后目标数据进行解密。而响应于数据使用方提交的数据获取交易, 区块链节点同样可以在可信执行环境中执行数据授权智能合约, 以在可信执行环境中生成授权令牌。因此, 通过在 TEE 中对目标数据进行加解密以及执行数据授权智能合约的代码, 可以确保提供安全可靠的环境, 避免受到外界因素的干扰。

[73] 除了存证于区块链节点的数据库之外, 目标数据可由数据所有方存储于链下渠道, 而区块链节点仅存储目标数据的数字摘要, 譬如该数字摘要可以为目标数据的哈希值。那么, 隐私计算平台可以向链下渠道获取目标数据, 并将目标数据和/或运算结果提供至数据使用方。

[74] 隐私计算平台在获得目标数据后, 可以将目标数据直接提供至数据使用方。或者, 隐私计算平台在获得目标数据后, 可以对目标数据执行预设运算, 并将运算结果提供至数据使用方。该预设运算可以为数据使用方希望采用的任意运算, 本说明书并不对此进行限制。例如, 该预设运算的运算规则可以被预定义于数据授权智能合约中; 其中, 该数据授权智能合约中可以定义一种或多种运算规则, 尤其是当存在多种运算规则时, 可由数据使用方在数据获取交易中指明所需采用的运算规则 (比如在数据获取交易的 data 字段添加该运算规则对应的标识等), 而数据授权智能合约可以将该所需采用的运算规

则添加于授权令牌中。再例如，该预设运算的运算规则可以由数据获取交易传入数据授权智能合约，比如可以将该预设运算的运算规则写入数据获取交易的 data 字段，进而传入数据授权智能合约中，而数据授权智能合约可以将该所需采用的运算规则添加于授权令牌中。又例如，该预设运算的运算规则可以由数据使用方随授权令牌一并提供至隐私计算平台。总之，隐私计算平台可以获知上述预设运算的运算规则，并基于该运算规则对目标数据实施预设运算，从而得到相应的运算结果并提供在数据使用方。当目标数据经由上述的预设运算得到相应的运算结果时，如果数据使用方无法由运算结果反推出目标数据的取值，就可以在满足数据使用方的数据获取需求的情况下，避免数据使用方直接获得目标数据，防止数据使用方对该目标数据造成外泄而侵犯数据所有方的权益，确保目标数据始终仅由数据所有方持有。

[75] 数据所有方持有的各个数据之间，可以存在不同的隐私级别；相应地，不同隐私级别的数据可以具有差异化的处理方式。例如，数据所有方可以分别持有隐私级别相对较低的数据和隐私级别相对较高的数据，即低隐私级别的数据和高隐私级别的数据；相应地，当目标数据属于低隐私级别时，该目标数据可以被提供至数据使用方，即数据所有方不关注低隐私级别的数据是否会发生外泄，而当目标数据属于高隐私级别时，目标数据需要被执行预设运算，以使相应的运算结果被提供至数据使用方，以确保高隐私级别的数据不会发生外泄。如果目标数据同时包含低隐私级别和高隐私级别的数据时，可以将低隐私级别的目标数据直接提供至数据使用方、将高隐私级别的目标数据经由预设运算后将运算结果提供至数据使用方；或者，可以将所有目标数据一并实施预设运算后，将运算结果提供至数据使用方。

[76] 出于对目标数据和/或运算结果的保护，隐私计算平台可以通过自身与数据使用方之间建立的数据通道(譬如加密数据通道)实现对目标数据和/或运算结果的传输。或者，隐私计算平台可以对目标数据和/或运算结果进行加密传输。在实施加密传输时，隐私计算平台可以采用数据使用方的公钥对目标数据和/或运算结果进行加密并传输至数据使用方，而数据使用方可以通过自身的私钥进行解密，以得到明文形式的目标数据和/或运算结果；或者，上述的授权令牌可以包含临时会话密钥，而目标数据和/或运算结果可以经由临时会话密钥加密后，由隐私计算平台传输至数据使用方。其中，授权令牌可以包括第一字段和第二字段，该第一字段的内容由数据使用方对应的第一密钥(如数据使用方的公钥)对临时会话密钥进行加密得到，该第二字段的内容由隐私计算平台对应的第二密钥(如隐私计算平台的公钥)对临时会话密钥进行加密得到，使得数据使用方、隐私计算平台可以分别从授权令牌中解密得到临时会话密钥，从而基于对称加密方案对目

标数据和/或运算结果进行加密传输。

[77] 相应地，图 4 是一示例性实施例提供的另一种基于区块链的数据授权方法的流程图。如图 4 所示，该方法应用于隐私计算平台，可以包括以下步骤：

[78] 步骤 402，隐私计算平台获取数据使用方提供的授权令牌，所述授权令牌由区块链上的数据授权智能合约向所述数据使用方颁发，表明所述数据使用方获得了对数据所有方持有的目标数据的授权。

[79] 如前所述，数据使用方可以通过向区块链网络提交数据获取交易来调用数据授权智能合约，使得该数据授权智能合约可以在确认数据使用方已获得授权时，向数据使用方颁发授权令牌。换言之，可以通过区块链网络上的数据授权智能合约，对数据使用方进行身份识别或权限验证，而隐私计算平台只需要识别授权令牌、无需关注于数据使用方的身份或权限。其中，数据授权智能合约确定数据所有方是否已获得授权的过程，可以参考图 3 所示的实施例，此处不再赘述。

[80] 步骤 404，所述隐私计算平台获取所述目标数据，以将所述目标数据和/或对所述目标数据执行预设运算后得到的运算结果返回至所述数据使用方。

[81] 目标数据可以存证于区块链上，譬如存储于区块链节点维护的数据库中。为了避免泄露目标数据，通常需要对目标数据进行加密后存储。例如，数据所有方可以向区块链网络中提交存证交易，该存证交易中包含加密后目标数据，使得区块链节点在收到存证交易后，可以对该存证交易中包含的加密后目标数据进行存储，其中加密后目标数据由数据所有方的公钥对目标数据进行加密后得到；相应地，数据所有方的私钥可以被托管于隐私计算平台处，使得隐私计算平台可以从区块链节点维护的数据库中读取加密后目标数据，并基于托管的数据所有方的私钥实施解密，以解密得到上述的目标数据。再例如，数据所有方可以向区块链网络中提交隐私存证交易，该隐私存证交易的交易内容处于加密状态且该交易内容包含目标数据，使得区块链节点可以在可信执行环境中解密得到该隐私存证交易的交易内容、得到目标数据，并采用数据所有方的公钥在可信执行环境中对目标数据进行加密，得到加密后目标数据，以存储于区块链节点对应的数据库中；相应地，数据所有方的私钥可以被托管于隐私计算平台处，以使隐私计算平台获得加密后目标数据后，可以通过该私钥解密得到上述的目标数据。又例如，目标数据可以由区块链节点在可信执行环境中执行某一区块链交易（比如数据所有方提交的存证交易）的过程中生成，而区块链节点可以采用数据所有方的公钥在可信执行环境中对生成的目标数据进行加密，得到加密后目标数据，以存储于区块链节点对应的数据库中；相应地，

数据所有方的私钥可以被托管于隐私计算平台处，以使隐私计算平台获得加密后目标数据后，可以通过该私钥解密得到上述的目标数据。

[82] 除了存证于区块链节点的数据库之外，目标数据可由数据所有方存储于链下渠道，而区块链节点仅存储目标数据的数字摘要，譬如该数字摘要可以为目标数据的哈希值。

5 那么，隐私计算平台可以根据授权令牌向链下渠道获取目标数据，并将目标数据和/或运算结果提供至数据使用方。

[83] 隐私计算平台在获得目标数据后，可以将目标数据直接提供至数据使用方。或者，隐私计算平台在获得目标数据后，可以对目标数据执行预设运算，并将运算结果提供至数据使用方。该预设运算可以为数据使用方希望采用的任意运算，本说明书并不对此进行限制。例如，该预设运算的运算规则可以被预定义于数据授权智能合约中；其中，该数据授权智能合约中可以定义一种或多种运算规则，尤其是当存在多种运算规则时，可由数据使用方在数据获取交易中指明所需采用的运算规则（比如在数据获取交易的 data 10 字段添加该运算规则对应的标识等），而数据授权智能合约可以将该所需采用的运算规则添加于授权令牌中。再例如，该预设运算的运算规则可以由数据获取交易传入数据授权智能合约，比如可以将该预设运算的运算规则写入数据获取交易的 data 字段，进而传入数据授权智能合约中，而数据授权智能合约可以将该所需采用的运算规则添加于授权令牌中。又例如，该预设运算的运算规则可以由数据使用方随授权令牌一并提供至隐私计算平台。总之，隐私计算平台可以获知上述预设运算的运算规则，并基于该运算规则对目标数据实施预设运算，从而得到相应的运算结果并提供在数据使用方。当目标数据 15 经由上述的预设运算得到相应的运算结果时，如果数据使用方无法由运算结果反推出目标数据的取值，就可以在满足数据使用方的数据获取需求的情况下，避免数据使用方直接获得目标数据，防止数据使用方对该目标数据造成外泄而侵犯数据所有方的权益，确保目标数据始终仅由数据所有方持有。

[84] 数据所有方持有的各个数据之间，可以存在不同的隐私级别；相应地，不同隐私 25 级别的数据可以具有差异化的处理方式。例如，数据所有方可以分别持有隐私级别相对较低的数据和隐私级别相对较高的数据，即低隐私级别的数据和高隐私级别的数据；相应地，当目标数据属于低隐私级别时，该目标数据可以被提供至数据使用方，即数据所有方不关注低隐私级别的数据是否会发生外泄，而当目标数据属于高隐私级别时，目标数据需要被执行预设运算，以使相应的运算结果被提供至数据使用方，以确保高隐私级别的数据不会发生外泄。如果目标数据同时包含低隐私级别和高隐私级别的数据时，可 30

以将低隐私级别的目标数据直接提供至数据使用方、将高隐私级别的目标数据经由预设运算后将运算结果提供至数据使用方；或者，可以将所有目标数据一并实施预设运算后，将运算结果提供至数据使用方。

[85] 出于对目标数据和/或运算结果的保护，隐私计算平台可以通过自身与数据使用方之间建立的数据通道(譬如加密数据通道)实现对目标数据和/或运算结果的传输。或者，隐私计算平台可以对目标数据和/或运算结果进行加密传输。在实施加密传输时，隐私计算平台可以采用数据使用方的公钥对目标数据和/或运算结果进行加密并传输至数据使用方，而数据使用方可以通过自身的私钥进行解密，以得到明文形式的目标数据和/或运算结果；或者，上述的授权令牌可以包含临时会话密钥，而目标数据和/或运算结果可以经由临时会话密钥加密后，由隐私计算平台传输至数据使用方。其中，授权令牌可以包括第一字段和第二字段，该第一字段的内容由数据使用方对应的第一密钥(如数据使用方的公钥)对临时会话密钥进行加密得到，该第二字段的内容由隐私计算平台对应的第二密钥(如隐私计算平台的公钥)对临时会话密钥进行加密得到，使得数据使用方、隐私计算平台可以分别从授权令牌中解密得到临时会话密钥，从而基于对称加密方案对目标数据和/或运算结果进行加密传输。

[86] 需要指出的是：本说明书中的由数据所有方持有、数据使用方请求的“数据”应当理解为一种广义概念，比如数值、文字、图像、音频、视频、代码、程序、模型(如人工智能模型)等，本说明书并不对此进行限制。

[87] 图 5 是一示例性实施例提供的一种基于区块链网络实现的端到端数据授权的示意图。如图 5 所示，假定在区块链网络中存在 N1、N2、N3、N4 和 N5 等节点，该区块链网络可以为服务平台与若干合作方组成的联盟链。例如，在供应链金融场景下，节点 N1、N2、N4 和 N5 等分别直接或间接对应于若干供应链金融企业，节点 N3 对应于服务平台，而用户可以基于该服务平台获取各个供应链金融企业的目标数据或基于目标数据得到的运算结果；再例如，在发票场景下，节点 N1、N2、N4 和 N5 等分别直接或间接对应于若干商家，节点 N3 对应于服务平台，而用户可以基于该服务平台获取各个商家开具的发票、发票中的部分信息或者基于发票信息得到的运算结果；当然，本说明书的技术方案还可以应用于其他场景，本说明书并不对此进行限制。为了便于理解，下面以发票场景为例进行描述。

[88] 假定用户 Ua(可以为个人或者机构)希望获取商家 CC 在最近 1 个月内开具的发票，那么本说明书的技术方案可使用户 Ua 便捷地获得这些发票，并保障这些发票的安

全性。例如，图 6 是一示例性实施例提供的一种基于区块链网络实现的端到端数据授权的交互流程图。如图 6 所示，用户 Ua、区块链节点、商家 CC 与链下平台之间的交互流程可以包括以下步骤：

[89] 步骤 601，用户 Ua 生成授权请求交易，并提交至区块链网络。

5 [90] 用户 Ua 使用的计算设备上可以运行客户端，并基于该客户端生成授权请求交易，以及提交至区块链网络。或者，用户 Ua 可以在客户端上生成授权请求交易后，将该授权请求交易上传至某一服务平台，由该服务平台将授权请求交易提交至区块链网络。或者，用户 Ua 可以向该服务平台发起授权请求，使得该服务平台生成授权请求交易，以及提交至区块链网络。

10 [91] 向区块链网络提交授权请求交易的目的，在于请求商家 CC 向该用户 Ua 赋予相关授权，使得用户 Ua 可以最终获得上述的最近 1 个月内开具的发票。授权请求交易中可以包含数据描述信息，以描述用户 Ua 希望分别向商家 CC 请求授权的数据，比如该数据描述信息可以用于描述商家 CC 最近 1 个月内开具的发票；相应地，用户 Ua 可以据此获得商家 CC 最近 1 个月内开具的发票的授权，但不会获得其他数据的授权。或者，
15 授权请求交易可以不包含数据描述信息，表明该用户 Ua 希望分别向商家 CC 请求获得对所有数据的授权，使得用户 Ua 对商家 CC 持有的所有数据均获得了授权，包括上述的最近 1 个月内开具的发票。下面以授权请求交易中包含数据描述信息为例，对后续步骤进行描述。

[92] 授权请求交易最初被提交至区块链网络中的某个节点，譬如图 5 所示的节点 N3 或其他节点。授权请求交易被提交至区块链网络后，可以在各个节点之间进行共识，而经过共识的授权请求交易可以在每个节点上分别执行。共识过程可以采用相关技术中的工作量证明（Proof of Work, POW）、股权证明（Proof of Stake, POS）、委任权益证明（Delegated Proof of Stake, DPOS）、实用拜占庭容错（Practical Byzantine Fault Tolerance, PBFT）或其他共识机制，本说明书并不对此进行限制。

20 [93] 步骤 602，区块链节点通过调用智能合约 TT 的请求接口，协助用户 Ua 获得数据授权，并在交易日志中写入授权请求事件。

[94] 经过共识后，区块链网络中的每个节点均需要执行上述的授权请求交易。区块链节点在执行授权请求交易时，通过读取该授权请求交易在 to 字段中填写的账户地址，调用智能合约 TT。其中，智能合约 TT 的代码可以在逻辑上形成多个接口，以分别实现不

同的功能，而授权请求交易中可以具体指明所需调用的接口。譬如，当授权请求交易调用了智能合约 TT 的请求接口时，可以据此请求获取相关授权。

[95] 例如，授权请求交易中可以包含前述的数据描述信息，以及用户 Ua 的信息（如用户 Ua 的签名）、商家 CC 的信息（如商家 CC 的公钥）等，使得智能合约 TT 的请求接口被调用后，可以在授权请求交易的交易日志中写入授权请求事件，该授权请求事件的内容可以包含上述的数据描述信息、用户 Ua 的信息、商家 CC 的信息等，表明用户 Ua 希望从商家 CC 处获得数据描述信息对应的目标数据。

[96] 步骤 603，商家 CC 监听授权请求事件。

[97] 由于所有区块链节点的操作一致，因而商家 CC 可以通过访问对应的任意区块链节点，即可基于事件监听机制获知上述的授权请求事件，以确定用户 Ua 希望从自身处获取的目标数据。

[98] 步骤 604，商家 CC 生成授权确认交易，并提交至区块链网络。

[99] 当商家 CC 同意用户 Ua 获取相关目标数据时，可以分别生成并提交授权确认交易，以表明自身同意向用户 Ua 提供诸如最近 1 个月开具的发票等目标数据。以商家 CC 为例：在商家 CC 生成的授权确认交易中，可以包含其自身同意向用户 Ua 提供的目标数据对应的数据描述信息、用户 Ua 的公钥、商家 CC 的签名等；或者，授权确认交易中

[100] 步骤 605，区块链节点调用智能合约 TT 的授权接口，更新用户 Ua 的授权状态，并在交易日志中写入授权状态更新事件。

[101] 如前所述，智能合约 TT 包含预定义的若干接口。在商家 CC 提交的授权确认交易中，to 字段可以分别包含智能合约 TT 的合约地址，并且可以指明希望调用授权接口。而智能合约 TT 可以通过运行授权接口对应的代码，确认商家 CC 分别同意向用户 Ua 赋予对诸如最近 1 个月开具的发票等目标数据的授权，从而将用户 Ua 的授权状态更新为已授权状态。如前所述，用户 Ua 的已授权状态可能采用多种形式进行记录，这取决于智能合约 TT 中定义的规则，此处不再赘述。

[102] 针对用户 Ua 的授权状态的更新情况，智能合约 TT 可以在交易日志中写入相应的授权状态更新事件，以表明用户 Ua 已经获得对于商家 CC 在最近 1 个月开具的发票的授权。

[103] 步骤 606, 用户 Ua 监听授权状态更新事件。

[104] 与步骤 603 相类似的, 用户 Ua 可以基于事件监听机制对区块链节点中对应于授权确认交易的交易日志进行监听, 并基于监听到的授权状态更新事件, 确定自身已经获得对于商家 CC 在最近 1 个月开具的发票的授权。

5 [105] 步骤 607, 用户 Ua 生成数据获取交易, 并提交至区块链网络。

[106] 与前述的授权请求交易相类似的, 用户 Ua 可以通过多种方式生成并提交数据获取交易, 比如独立生成并提交、独立生成后由服务平台提交、由服务平台生成并提交等, 此处不再赘述。

10 [107] 数据获取交易中可以包含数据描述信息, 以描述用户 Ua 希望获得商家 CC 在最近 1 个月开具的发票; 或者, 数据获取交易中可以包含前述的授权请求交易的交易编号或者前述的授权确认交易的交易编号, 同样可以间接表明希望获取商家 CC 在最近 1 个月开具的发票。

[108] 步骤 608, 区块链节点调用智能合约 TT 的数据接口, 生成授权令牌并在交易日志中添加该授权令牌。

15 [109] 通过调用智能合约 TT 的数据接口, 可以向智能合约 TT 表明: 用户 Ua 希望获取商家 CC 在最近 1 个月开具的发票。那么, 智能合约 TT 可以查询用户 Ua 的授权状态。

[110] 如果用户 Ua 并未获得授权, 可以终止交易; 或者, 智能合约 TT 可以向交易日志中写入授权请求事件, 从而通过类似于步骤 602~605 的过程, 临时向商家 CC 请求授权, 此时数据获取交易相当于同时实现了授权请求和数据获取的功能, 可以省去前述授权请求交易的相关操作和步骤。

20

[111] 如果用户 Ua 已获得授权, 智能合约 TT 可以为用户 Ua 生成授权令牌, 使得用户 Ua 可以基于该授权令牌获得商家 CC 在最近 1 个月开具的发票。图 7 是一示例性实施例提供的一种授权令牌的示意图; 如图 7 所示, 授权令牌可以包含用户 ID、 $ENC(K_{Ua}, K_{TEMP})$ 、 $ENC(K_M, K_{TEMP})$ 、授权内容、TAG 等若干字段; 当然, 授权令牌的内容可以随场景差异而存在适当变化, 本说明书并不对此进行限制。

25

[112] 用户 ID 字段可以包含用户 Ua 的 ID。那么, 当用户 Ua 在后续将该授权令牌提供至链下平台时, 链下平台可以对提供方的信息和该授权令牌所含的用户 ID 进行比较, 并将比较结果一致作为授权令牌通过验证的条件之一。换言之, 如果该授权令牌被用户 Ub 获得, 并且用户 Ub 将该授权令牌提供至链下平台时, 由于该授权令牌所含的用户 ID

属于用户 U_a 、区别于用户 U_b ，因而链下平台可以判定该授权令牌未通过验证，即该授权令牌无效；如果用户 U_a 将该授权令牌提供至链下平台，那么由于该授权令牌的用户 ID 字段包含该用户 U_a 的 ID，因而可以确定授权令牌的提供者与授权令牌一致，授权令牌有效。

- 5 [113] $ENC(K_{U_a}, K_{TEMP})$ 表示的含义为：采用预设算法对 K_{U_a} 和 K_{TEMP} 进行加密得到的加密结果。其中， K_{U_a} 为对应于用户 U_a 的密钥， K_{TEMP} 为智能合约 TT 针对本次数据授权生成的临时密钥；其中， K_{U_a} 由用户 U_a 掌握，使得用户 U_a 可以基于密钥 K_{U_a} 对 $ENC(K_{U_a}, K_{TEMP})$ 进行解密，从而得到临时密钥 K_{TEMP} 。

- 10 [114] $ENC(K_M, K_{TEMP})$ 表示的含义为：采用预设算法对 K_M 和 K_{TEMP} 进行加密得到的加密结果。其中， K_M 为对应于链下平台的密钥， K_{TEMP} 为智能合约 TT 针对本次数据授权生成的临时密钥；其中， K_M 由链下平台掌握，使得链下平台可以基于密钥 K_M 对 $ENC(K_M, K_{TEMP})$ 进行解密，从而得到临时密钥 K_{TEMP} 。

[115] 授权内容可以包含上述的数据描述信息，以用于描述用户 U_a 获得授权的数据。例如，在如图 6 所示的实施例，授权内容可以为商家 CC 在最近 1 个月开具的发票。

- 15 [116] TAG 字段用于验证授权令牌的内容完整性和真实性。除了 TAG 字段之外，假定前述的用户 ID、 $ENC(K_{U_a}, K_{TEMP})$ 、 $ENC(K_M, K_{TEMP})$ 和授权内容等字段的内容统称为 MG，那么 TAG 字段的内容可以包括 $MAC=C(K_M, MG)$ ，即根据密钥和内容 MG 生成的消息认证码 (Message Authentication Code, 简称 MAC)，其中 $C()$ 表示所采用的生成函数。那么，链下平台在收到授权令牌后，可以根据自身掌握的密钥 K_M 和 TAG 字段所含的
- 20 MAC，对授权令牌所含的其他字段进行验证，以确定是否内容 MG 被篡改或者在传输过程中发生了数据丢失、损坏等。

[117] 步骤 609，用户 U_a 监听交易执行结果事件。

- [118] 如前所述，用户 U_a 可以基于事件监听回调机制对数据获取交易的交易日志进行监听，以监听到交易执行结果事件。如果数据获取交易顺利实施，那么用户 U_a 可以从该
- 25 交易执行结果事件中获得授权令牌。

[119] 步骤 610，链下平台收到用户 U_a 发送的授权令牌，并针对授权令牌进行验证。

[120] 如前所述，链下平台可以根据 TAG 字段针对授权令牌的完整性进行验证，对用户 ID 字段与用户 U_a 之间的一致性进行验证等。如果全部验证无误，链下平台可以从授权令牌中解密得到临时密钥 K_{TEMP} 。

[121] 步骤 611, 在验证无误后, 链下平台从区块链上获取加密后发票。

[122] 步骤 612, 链下平台对加密后发票进行解密后, 将发票返回至用户 Ua。

[123] 通过将加密后发票存证于区块链上, 使得链下平台可以对区块链网络中的任意区块链节点进行访问, 并获得该加密后发票; 实际上, 由于区块链网络上存证的所有数据全部处于公开状态, 因而链下平台可以对区块链网络上存证的数据进行随意访问。甚至, 链下平台可以将区块链网络上的数据同步至本地, 使得在获得用户 Ua 提供的授权令牌后, 可以直接从本地获得加密后发票、无需临时访问区块链网络, 可以加快响应速度、缩短用户 Ua 的等待时长。

[124] 发票可以采用商家 CC 的公钥进行加密, 以得到上述的加密后发票。该加密后发票仅能够通过商家 CC 的私钥进行解密, 并且该私钥并不处于公开状态, 因而即便加密后发票可以被随意访问, 也可以确保商家 CC 的发票处于安全状态。而为了满足授权用户对发票的获取需求, 同时减轻商家 CC 的处理压力, 可由链下平台向商家 CC 提供私钥托管服务, 使得商家 CC 可以将私钥安全托管于链下平台处, 那么链下平台可以直接对加密后发票进行解密, 并将解密得到的发票提供至诸如用户 Ua 等数据使用方。

[125] 在解密得到明文的发票后, 链下平台可以采用前述的临时密钥 K_{TEMP} 对发票进行加密后, 传输至用户 Ua; 相应的, 用户 Ua 可以采用临时密钥 K_{TEMP} 对收到的传输数据进行解密, 即可得到商家 CC 在最近 1 个月开具的发票, 从而确保在链下平台与用户 Ua 之间实现安全的数据传输。

[126] 在如图 5-6 所示的实施例, 数据所有方持有的数据采用公钥进行加密后存证于区块链网络中, 比如可以存证于区块中 (包含于交易内容中) 或者存证于区块链节点维护的本地数据库中, 并通过将数据所有方的私钥托管于链下平台处, 使得链下平台可以直接向数据使用方提供其需要的数据。而在其他实施例, 数据所有方可以将相关数据存证于链下存储空间而非区块链网络中, 使得链下平台需要与链下存储空间进行交易, 以获得相应的目标数据。例如, 图 8 是一示例性实施例提供的另一种基于区块链网络实现的端到端数据授权的示意图。如图 8 所示, 区块链网络的相关结构与图 5 相似, 此处不再赘述。假定用户 Ua 希望获取商家 CC 在最近 3 个月所开发票的平均开票额, 那么存在两种方式: 1) 将商家 CC 在最近 3 个月开具的发票均提供至用户 Ua, 由用户 Ua 计算平均开票额; 2) 计算出商家 CC 在最近 3 个月所开发票的平均开票额后, 仅将平均开票额提供至用户 Ua。

[127] 方式 1) 类似于图 5-6 所示的实施例, 只是图 8 中的交互过程存在一些差异。如图 8 所示, 用户 Ua 可以通过诸如图 6 中的步骤 601~609 获得授权令牌, 该授权令牌的授权内容字段描述了商家 CC 在最近 3 个月开具的发票。用户 Ua 将授权令牌提供至链下平台 81, 链下平台 81 可以在确定该授权令牌通过验证后, 向链下存储空间 82 请求获取商家 CC 在最近 3 个月开具的发票; 其中, 该链下存储空间 82 可由商家 CC 维护, 或者由商家 CC 之外的其他对象所维护。然后, 链下平台 81 基于如前所述的临时密钥 K_{TEMP} 对发票数据进行加密后, 传输至用户 Ua; 以及, 用户 Ua 采用临时密钥 K_{TEMP} 进行加密后, 可以对得到的发票数据做进一步计算, 以得到相应的平均开票额。

[128] 方式 2) 则存在较大差异。如图 8 所示, 用户 Ua 可以通过诸如图 6 中的步骤 601~609 获得授权令牌, 该授权令牌的授权内容字段描述了商家 CC 在最近 3 个月所开发票的平均开票额, 使得用户 Ua 将授权令牌提供至链下平台 81, 链下平台 81 可以在确定该授权令牌通过验证后, 向链下存储空间 82 请求获取商家 CC 在最近 3 个月开具的发票, 并且由链下平台 81 基于这些发票计算出相应的平均开票额。然后, 链下平台 81 基于如前所述的临时密钥 K_{TEMP} 对平均开票额进行加密后, 传输至用户 Ua; 以及, 用户 Ua 采用临时密钥 K_{TEMP} 进行加密后, 即可得到平均开票额。基于方式 2), 可使用户 Ua 获得平均开票额的取值, 并且不会向用户 Ua 暴露每张发票的开票额, 从而既能够满足用户 Ua 的需求, 又能够避免商家 CC 的发票数据产生外泄, 尤其是可以避免用户 Ua 在获得发票后将其进一步提供至其他用户, 确保商家 CC 所持的数据处于安全可控的状态。

[129] 上述方式 2) 中所采用的处理方式同样可以适用于图 5-6 所示的实施例。例如, 链下平台 50 可以从区块链网络中获得商家 CC 在最近 3 个月开具的发票对应的加密后数据, 并基于托管的私钥解密得到明文的发票, 然后由链下平台 50 计算得到商家 CC 在最近 3 个月所开发票的平均开票额, 并将该平均开票额提供至用户 Ua, 避免用户 Ua 直接接触到商家 CC 在最近 3 个月开具的发票。

[130] 图 9 是一示例性实施例提供的一种设备的示意结构图。请参考图 9, 在硬件层面, 该设备包括处理器 902、内部总线 904、网络接口 906、内存 908 以及非易失性存储器 910, 当然还可能包括其他业务所需要的硬件。处理器 902 从非易失性存储器 910 中读取对应的计算机程序到内存 908 中然后运行, 在逻辑层面上形成基于区块链的数据授权装置。当然, 除了软件实现方式之外, 本说明书一个或多个实施例并不排除其他实现方式, 比如逻辑器件抑或软硬件结合的方式等等, 也就是说以下处理流程的执行主体并不限定于各个逻辑单元, 也可以是硬件或逻辑器件。

[131] 请参考图 10, 在软件实施方式中, 该基于区块链的数据授权装置可以包括:

[132] 接收单元 1001, 使区块链节点接收数据使用方提交的数据获取交易, 所述数据获取交易用于请求获取数据所有方持有的目标数据;

5 [133] 执行单元 1002, 使所述区块链节点执行所述数据获取交易调用的数据授权智能合约, 所述数据授权智能合约用于在确认所述数据使用方已获得授权时, 向所述数据使用方颁发授权令牌; 所述授权令牌被所述数据使用方提供至隐私计算平台后, 用于指示所述隐私计算平台获取所述目标数据, 并将所述目标数据和/或对所述目标数据执行预设运算后得到的运算结果返回至所述数据使用方。

10 [134] 可选的, 所述数据授权智能合约存在对应的授权方名单; 其中, 所述数据授权智能合约在确认所述数据使用方位于所述授权方名单内时, 确认所述数据使用方已获得授权。

[135] 可选的, 还包括:

15 [136] 请求单元 1003, 使所述区块链节点根据所述数据使用方提交的授权请求交易, 调用所述数据授权智能合约中定义的请求接口, 使所述数据授权智能合约在交易日志中写入授权请求事件, 以由所述数据所有方进行监听;

[137] 授权单元 1004, 使所述区块链节点根据所述数据所有方提交的授权确认交易, 调用所述数据授权智能合约中定义的授权接口, 使所述数据授权智能合约确认所述数据使用方已获得授权。

20 [138] 可选的, 所述数据授权智能合约还用于在完成授权令牌的颁发操作后, 取消所述数据使用方的已授权状态; 或者, 所述数据授权智能合约还用于在完成授权令牌的颁发操作后, 递减所述数据使用方对应的剩余授权次数。

[139] 可选的, 当所述目标数据属于低隐私级别时, 所述目标数据被提供至所述数据使用方; 当所述目标数据属于高隐私级别时, 所述目标数据被执行所述预设运算, 以使相应的运算结果被提供至所述数据使用方。

25 [140] 可选的, 还包括:

[141] 存储单元 1005, 使所述区块链节点在收到存证交易后, 对所述存证交易中包含的加密后目标数据进行存储, 所述加密后目标数据由所述数据所有方的公钥对所述目标数据进行加密后得到;

[142] 其中，所述数据所有方的私钥被托管于所述隐私计算平台处，以使所述隐私计算平台获得所述加密后目标数据后，解密得到所述目标数据。

[143] 可选的，还包括：

5 [144] 加密单元 1006，使所述区块链节点采用所述数据所有方的公钥在可信执行环境中对所述目标数据进行加密，得到加密后目标数据，以存储于所述区块链节点对应的数据库中；

[145] 其中，所述数据所有方的私钥被托管于所述隐私计算平台处，以使所述隐私计算平台获得所述加密后目标数据后，解密得到所述目标数据。

[146] 可选的，还包括：

10 [147] 解密单元 1007，使所述区块链节点在收到所述数据所有方提交的隐私存证交易后，在所述可信执行环境中对所述隐私存证交易进行解密，以得到交易内容中包含的所述目标数据；

[148] 或者，生成单元 1008，使所述区块链节点在收到所述数据所有方提交的存证交易后，在所述可信执行环境中执行相应的交易内容，以生成所述目标数据。

15 [149] 可选的，所述区块链节点存储了所述目标数据的数字摘要，所述目标数据由所述数据所有方存储于链下渠道；其中，所述目标数据由所述隐私计算平台向所述链下渠道获取。

[150] 可选的，所述授权令牌包含临时会话密钥，所述目标数据和/或所述运算结果经由所述临时会话密钥加密后，由所述隐私计算平台传输至所述数据使用方。

20 [151] 可选的，所述授权令牌包括第一字段和第二字段，所述第一字段的内容由所述数据使用方对应的第一密钥对所述临时会话密钥进行加密得到，所述第二字段的内容由所述隐私计算平台对应的第二密钥对所述临时会话密钥进行加密得到。

[152] 图 11 是一示例性实施例提供的一种设备的示意结构图。请参考图 11，在硬件层面，该设备包括处理器 1102、内部总线 1104、网络接口 1106、内存 1108 以及非易失性存储器 1110，当然还可能包括其他业务所需要的硬件。处理器 1102 从非易失性存储器 1110 中读取对应的计算机程序到内存 1108 中然后运行，在逻辑层面上形成基于区块链的数据授权装置。当然，除了软件实现方式之外，本说明书一个或多个实施例并不排除其他实现方式，比如逻辑器件抑或软硬件结合的方式等等，也就是说以下处理流程的执行主

25

体并不限于各个逻辑单元，也可以是硬件或逻辑器件。

[153] 请参考图 12，在软件实施方式中，该基于区块链的数据授权装置可以包括：

[154] 令牌获取单元 1201，使隐私计算平台获取数据使用方提供的授权令牌，所述授权令牌由区块链上的数据授权智能合约向所述数据使用方颁发，表明所述数据使用方获得了对数据所有方持有的目标数据的授权；

[155] 数据获取单元 1202，使所述隐私计算平台获取所述目标数据，以将所述目标数据和/或对所述目标数据执行预设运算后得到的运算结果返回至所述数据使用方。

[156] 可选的，所述数据获取单元 1202 具体用于：

[157] 使所述隐私计算平台从区块链节点处获得加密后目标数据，所述加密后目标数据由所述数据所有方的公钥对所述目标数据进行加密后得到；

[158] 使所述隐私计算平台采用托管的所述数据所有方的私钥对所述加密后目标数据进行解密，以得到所述目标数据。

[159] 可选的，所述区块链节点存储了所述目标数据的数字摘要，所述目标数据由所述数据所有方存储于链下渠道；所述数据获取单元 1202 具体用于：

[160] 使所述隐私计算平台向所述链下渠道提供所述目标数据的数字摘要；

[161] 使所述隐私计算平台接收所述链下渠道返回的所述目标数据。

[162] 上述实施例阐明的系统、装置、模块或单元，具体可以由计算机芯片或实体实现，或者由具有某种功能的产品来实现。一种典型的实现设备为计算机，计算机的具体形式可以是个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件收发设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任意几种设备的组合。

[163] 在一个典型的配置中，计算机包括一个或多个处理器 (CPU)、输入/输出接口、网络接口和内存。

[164] 内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器 (RAM) 和/或非易失性内存等形式，如只读存储器 (ROM) 或闪存(flash RAM)。内存是计算机可读介质的示例。

[165] 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数

据。计算机的存储介质的例子包括，但不限于相变内存 (PRAM)、静态随机存取存储器 (SRAM)、动态随机存取存储器 (DRAM)、其他类型的随机存取存储器 (RAM)、只读存储器 (ROM)、电可擦除可编程只读存储器 (EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器 (CD-ROM)、数字多功能光盘 (DVD) 或其他光学存储、磁盒式磁带、磁盘存储、量子存储器、基于石墨烯的存储介质或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括暂存电脑可读媒体 (transitory media)，如调制的数据信号和载波。

[166] 还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

[167] 上述对本说明书特定实施例进行了描述。其它实施例在所附权利要求书的范围内。在一些情况下，在权利要求书中记载的动作或步骤可以按照不同于实施例中的顺序来执行并且仍然可以实现期望的结果。另外，在附图中描绘的过程不一定要求示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中，多任务处理和并行处理也是可以的或者可能是有利的。

[168] 在本说明书一个或多个实施例使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本说明书一个或多个实施例。在本说明书一个或多个实施例和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式，除非上下文清楚地表示其他含义。还应当理解，本文中使用的术语“和/或”是指并包含一个或多个相关联的列出项目的任何或所有可能组合。

[169] 应当理解，尽管在本说明书一个或多个实施例可能采用术语第一、第二、第三等来描述各种信息，但这些信息不应限于这些术语。这些术语仅用来将同一类型的信息彼此区分开。例如，在不脱离本说明书一个或多个实施例范围的情况下，第一信息也可以被称为第二信息，类似地，第二信息也可以被称为第一信息。取决于语境，如在此所使用的词语“如果”可以被解释成为“在……时”或“当……时”或“响应于确定”。

[170] 以上所述仅为本说明书一个或多个实施例的较佳实施例而已，并不用以限制本说明书一个或多个实施例，凡在本说明书一个或多个实施例的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本说明书一个或多个实施例保护的范围之内。

权利要求书

1. 一种基于区块链的数据授权方法，包括：

区块链节点接收数据使用方提交的数据获取交易，所述数据获取交易用于请求获取数据所有方持有的目标数据；

5 所述区块链节点执行所述数据获取交易调用的数据授权智能合约，所述数据授权智能合约用于在确认所述数据使用方已获得授权时，向所述数据使用方颁发授权令牌；所述授权令牌被所述数据使用方提供至隐私计算平台后，用于指示所述隐私计算平台获取所述目标数据，并将所述目标数据和/或对所述目标数据执行预设运算后得到的运算结果返回至所述数据使用方。

10 2. 根据权利要求 1 所述的方法，所述数据授权智能合约存在对应的授权方名单；其中，所述数据授权智能合约在确认所述数据使用方位于所述授权方名单内时，确认所述数据使用方已获得授权。

3. 根据权利要求 1 所述的方法，还包括：

15 所述区块链节点根据所述数据使用方提交的授权请求交易，调用所述数据授权智能合约中定义的请求接口，使所述数据授权智能合约在交易日志中写入授权请求事件，由所述数据所有方进行监听；

所述区块链节点根据所述数据所有方提交的授权确认交易，调用所述数据授权智能合约中定义的授权接口，使所述数据授权智能合约确认所述数据使用方已获得授权。

20 4. 根据权利要求 3 所述的方法，所述数据授权智能合约还用于在完成授权令牌的颁发操作后，取消所述数据使用方的已授权状态；或者，所述数据授权智能合约还用于在完成授权令牌的颁发操作后，递减所述数据使用方对应的剩余授权次数。

5. 根据权利要求 1 所述的方法，当所述目标数据属于低隐私级别时，所述目标数据被提供至所述数据使用方；当所述目标数据属于高隐私级别时，所述目标数据被执行所述预设运算，以使相应的运算结果被提供至所述数据使用方。

25 6. 根据权利要求 1 所述的方法，还包括：

所述区块链节点在收到存证交易后，对所述存证交易中包含的加密后目标数据进行存储，所述加密后目标数据由所述数据所有方的公钥对所述目标数据进行加密后得到；

其中，所述数据所有方的私钥被托管于所述隐私计算平台处，以使所述隐私计算平台获得所述加密后目标数据后，解密得到所述目标数据。

30 7. 根据权利要求 1 所述的方法，还包括：

所述区块链节点采用所述数据所有方的公钥在可信执行环境中对所述目标数据进行加密，得到加密后目标数据，以存储于所述区块链节点对应的数据库中；

其中,所述数据所有方的私钥被托管于所述隐私计算平台处,以使所述隐私计算平台获得所述加密后目标数据后,解密得到所述目标数据。

8. 根据权利要求 7 所述的方法,还包括:

所述区块链节点在收到所述数据所有方提交的隐私存证交易后,在所述可信执行环境中对所述隐私存证交易进行解密,以得到交易内容中包含的所述目标数据;

或者,所述区块链节点在收到所述数据所有方提交的存证交易后,在所述可信执行环境中执行相应的交易内容,以生成所述目标数据。

9. 根据权利要求 1 所述的方法,所述区块链节点存储了所述目标数据的数字摘要,所述目标数据由所述数据所有方存储于链下渠道;其中,所述目标数据由所述隐私计算平台向所述链下渠道获取。

10. 根据权利要求 1 所述的方法,所述授权令牌包含临时会话密钥,所述目标数据和/或所述运算结果经由所述临时会话密钥加密后,由所述隐私计算平台传输至所述数据使用方。

11. 根据权利要求 10 所述的方法,所述授权令牌包括第一字段和第二字段,所述第一字段的内容由所述数据使用方对应的第一密钥对所述临时会话密钥进行加密得到,所述第二字段的内容由所述隐私计算平台对应的第二密钥对所述临时会话密钥进行加密得到。

12. 一种基于区块链的数据授权方法,包括:

隐私计算平台获取数据使用方提供的授权令牌,所述授权令牌由区块链上的数据授权智能合约向所述数据使用方颁发,表明所述数据使用方获得了对数据所有方持有的目标数据的授权;

所述隐私计算平台获取所述目标数据,以将所述目标数据和/或对所述目标数据执行预设运算后得到的运算结果返回至所述数据使用方。

13. 根据权利要求 12 所述的方法,所述隐私计算平台获取所述目标数据,包括:

所述隐私计算平台从区块链节点处获得加密后目标数据,所述加密后目标数据由所述数据所有方的公钥对所述目标数据进行加密后得到;

所述隐私计算平台采用托管的所述数据所有方的私钥对所述加密后目标数据进行解密,以得到所述目标数据。

14. 根据权利要求 12 所述的方法,所述区块链节点存储了所述目标数据的数字摘要,所述目标数据由所述数据所有方存储于链下渠道;所述隐私计算平台获取所述目标数据,包括:

所述隐私计算平台向所述链下渠道提供所述目标数据的数字摘要;

所述隐私计算平台接收所述链下渠道返回的所述目标数据。

15. 一种基于区块链的数据授权装置，包括：

接收单元，使区块链节点接收数据使用方提交的数据获取交易，所述数据获取交易用于请求获取数据所有方持有的目标数据；

5 执行单元，使所述区块链节点执行所述数据获取交易调用的数据授权智能合约，所述数据授权智能合约用于在确认所述数据使用方已获得授权时，向所述数据使用方颁发授权令牌；所述授权令牌被所述数据使用方提供至隐私计算平台后，用于指示所述隐私计算平台获取所述目标数据，并将所述目标数据和/或对所述目标数据执行预设运算后得到的运算结果返回至所述数据使用方。

10 16. 一种基于区块链的数据授权装置，包括：

令牌获取单元，使隐私计算平台获取数据使用方提供的授权令牌，所述授权令牌由区块链上的数据授权智能合约向所述数据使用方颁发，表明所述数据使用方获得了对数据所有方持有的目标数据的授权；

15 数据获取单元，使所述隐私计算平台获取所述目标数据，以将所述目标数据和/或对所述目标数据执行预设运算后得到的运算结果返回至所述数据使用方。

17. 一种电子设备，包括：

处理器；

用于存储处理器可执行指令的存储器；

20 其中，所述处理器通过运行所述可执行指令以实现如权利要求 1-11 中任一项所述的方法。

18. 一种计算机可读存储介质，其上存储有计算机指令，该指令被处理器执行时实现如权利要求 1-11 中任一项所述方法的步骤。

19. 一种电子设备，包括：

处理器；

25 用于存储处理器可执行指令的存储器；

其中，所述处理器通过运行所述可执行指令以实现如权利要求 12-14 中任一项所述的方法。

20. 一种计算机可读存储介质，其上存储有计算机指令，该指令被处理器执行时实现如权利要求 12-14 中任一项所述方法的步骤。

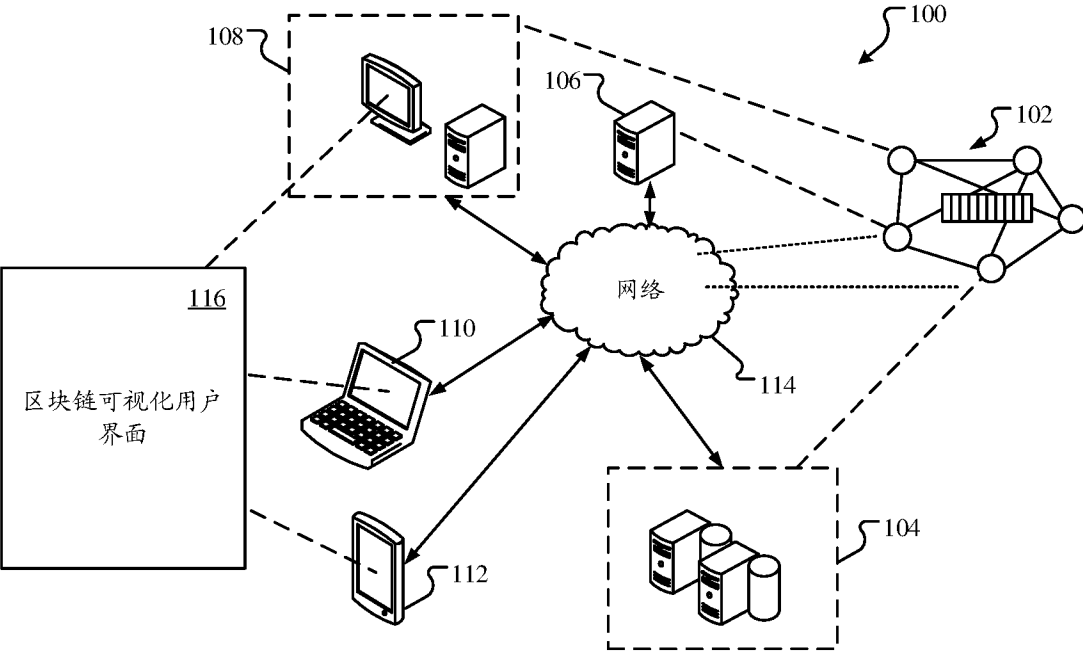


图 1

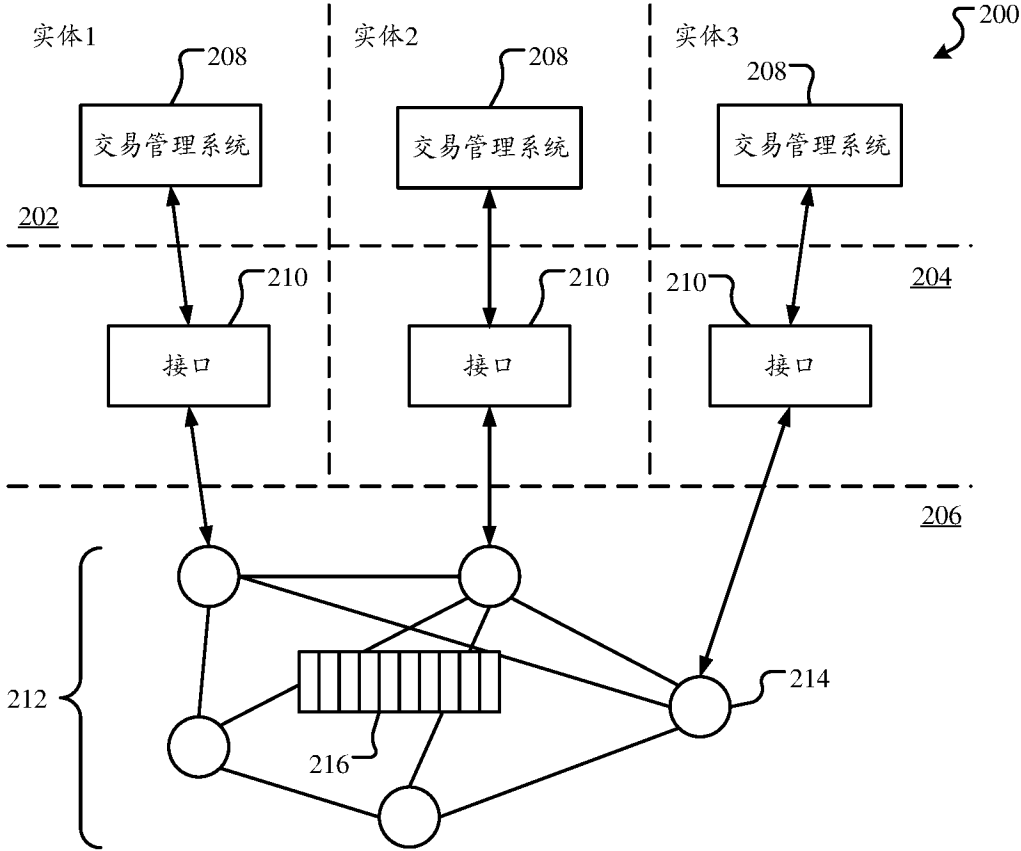


图 2

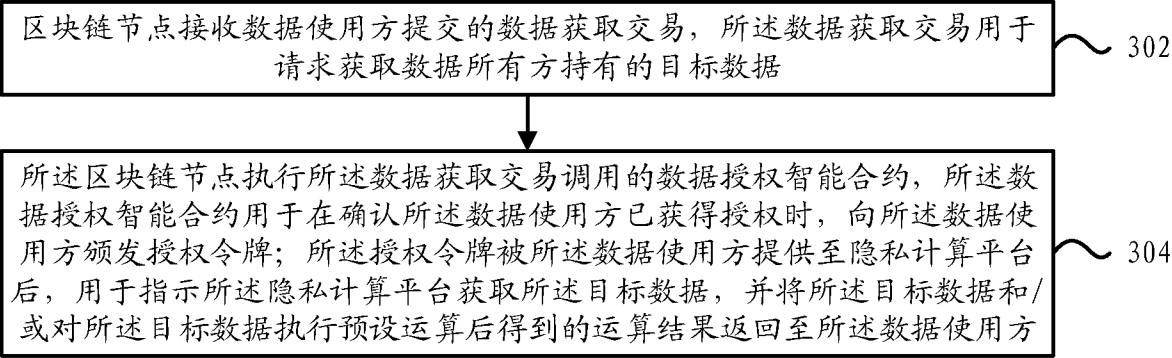


图 3

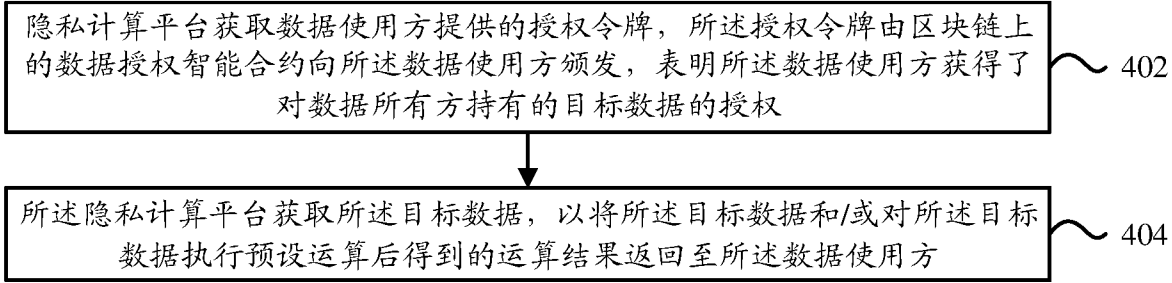


图 4

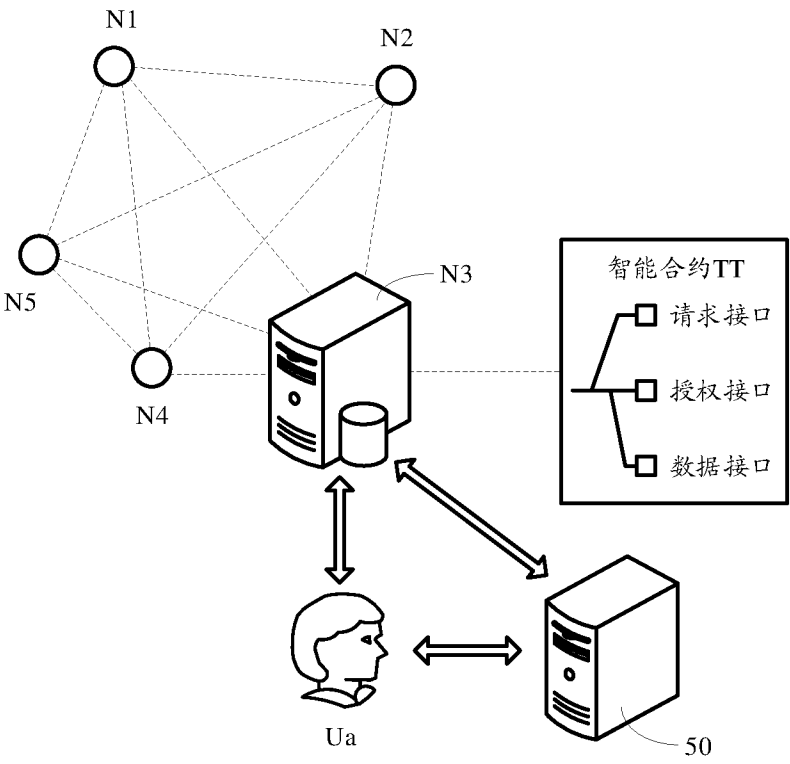


图 5

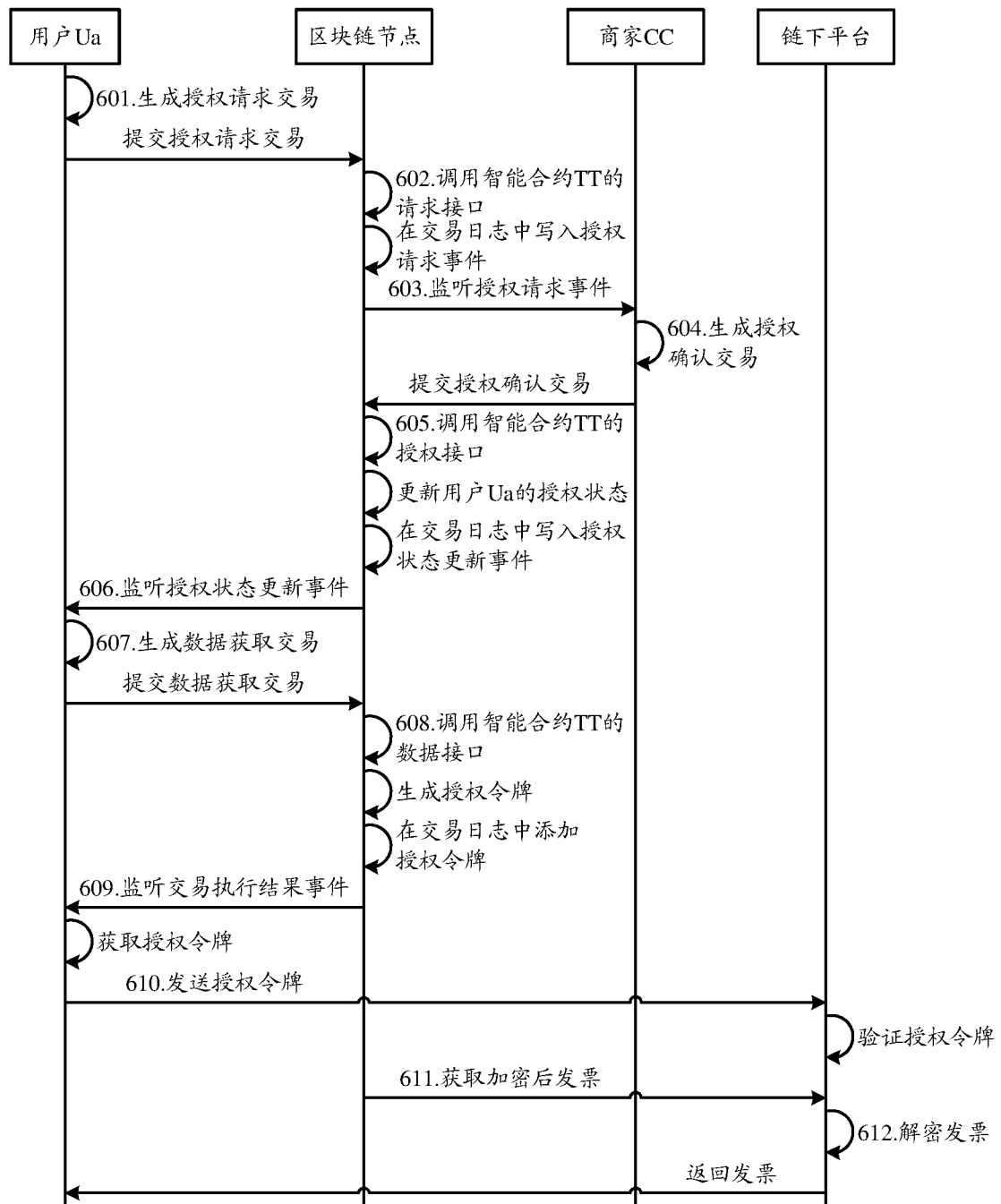


图 6

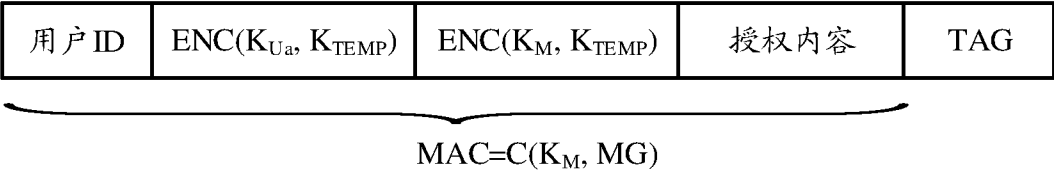


图 7

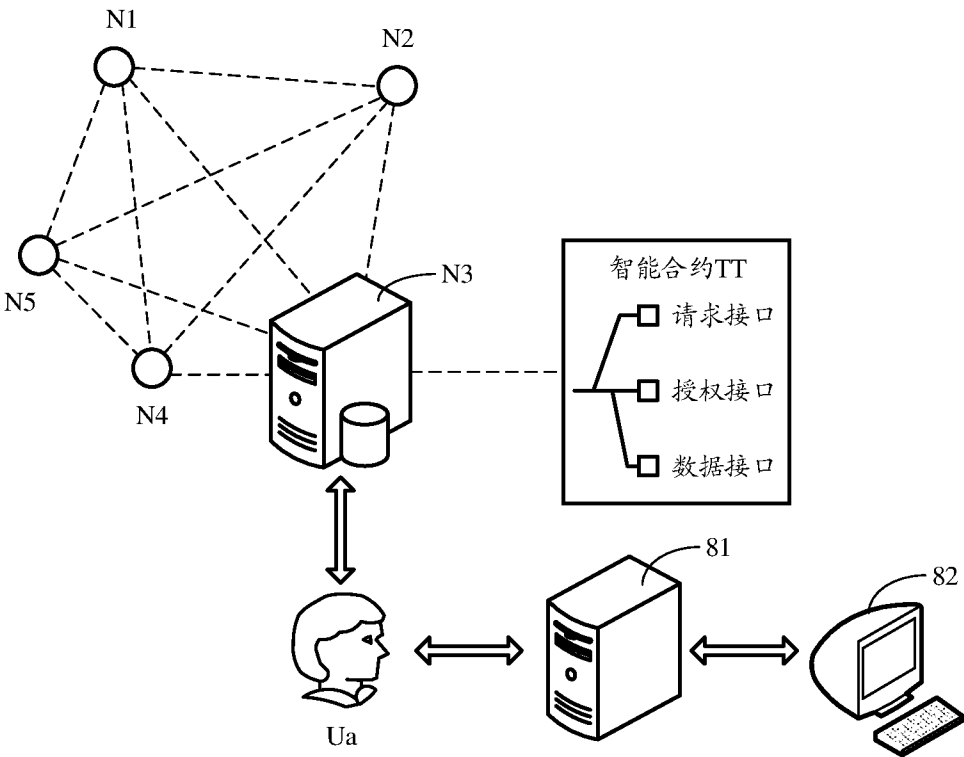


图 8

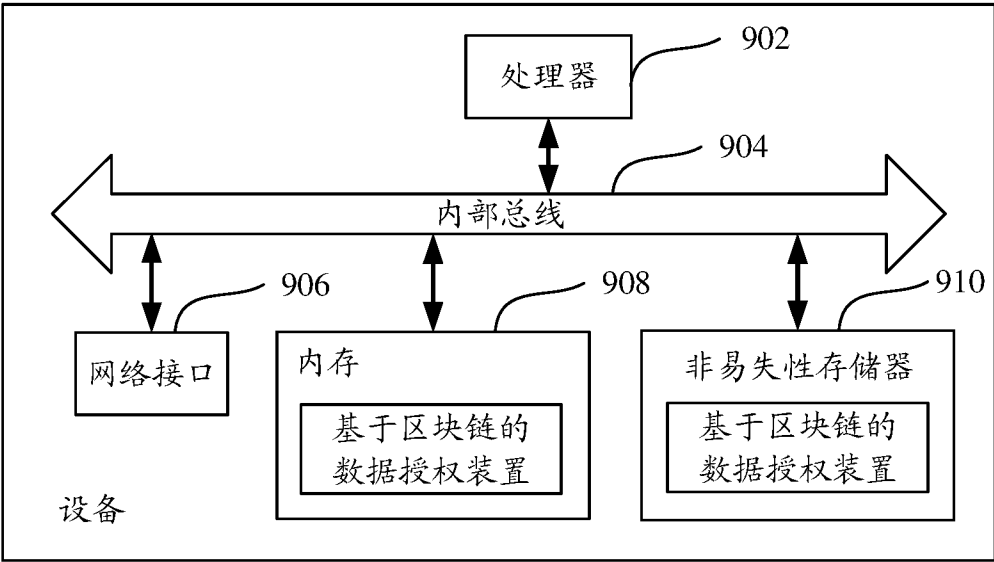


图 9

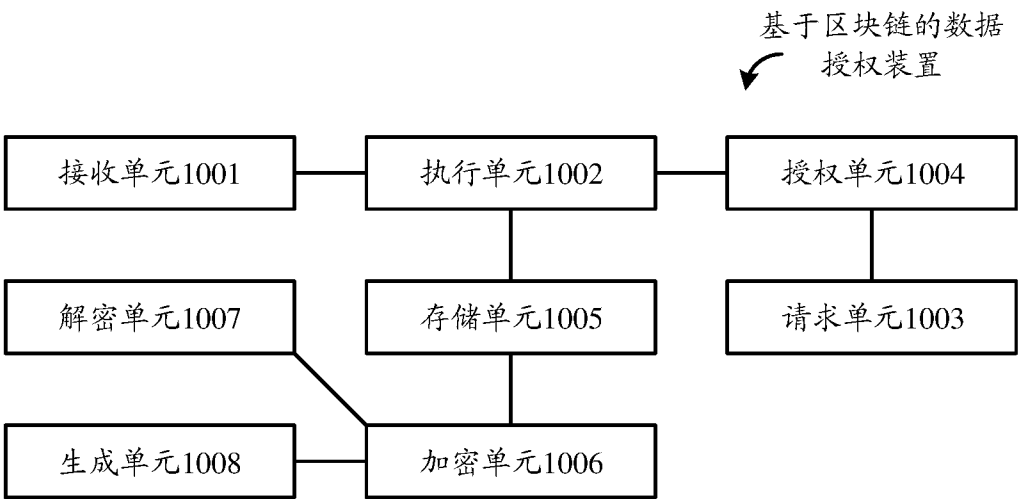


图 10

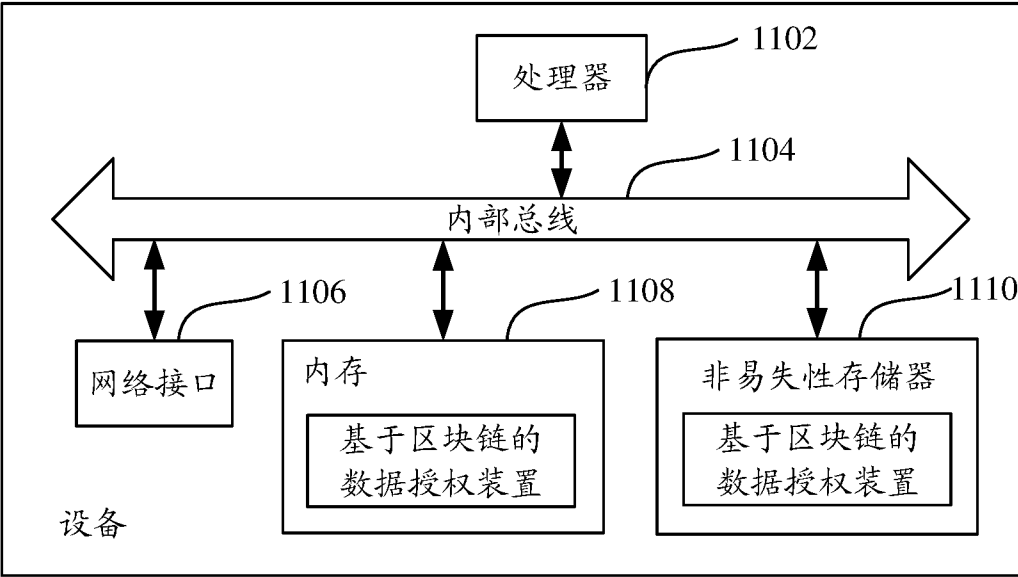


图 11

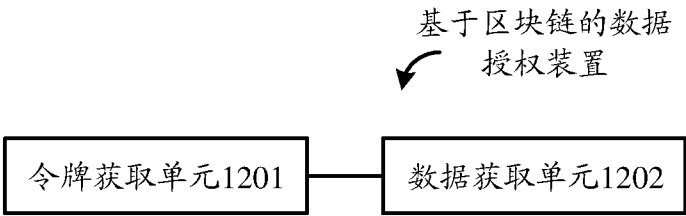


图 12

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2020/072153

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/30(2013.01)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)

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; CNABS; CNKI; TWTXT; TWABS; USTXT; VEN; EPTXT; WOTXT: 区块链, 授权, 智能合约, 智能合同, 令牌, 节点, 数据, 交易, 加密, block chain, blockchain, authorization, smart contract, token, node, data, transaction, encrypt

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110457875 A (ALIBABA GROUP HOLDING LIMITED) 15 November 2019 (2019-11-15) entire document	1-20
X	WO 2019078879 A1 (HEWLETT PACKARD ENTERPRISE DEVELOPMENT LP) 25 April 2019 (2019-04-25) description, paragraphs 10-70, figures 1-5	1-20
A	CN 110011996 A (ALIBABA GROUP HOLDING LIMITED) 12 July 2019 (2019-07-12) entire document	1-20
A	CN 109639643 A (PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) 16 April 2019 (2019-04-16) 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

27 April 2020

Date of mailing of the international search report

08 May 2020

Name and mailing address of the ISA/CN

China National Intellectual Property Administration (ISA/
CN)
No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing
100088
China

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2020/072153

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN	110457875	A	15 November 2019	None	
WO	2019078879	A1	25 April 2019	None	
CN	110011996	A	12 July 2019	None	
CN	109639643	A	16 April 2019	None	

国际检索报告

国际申请号

PCT/CN2020/072153

A. 主题的分类

G06F 21/30 (2013.01) 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)

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;CNABS;CNKI;TWTXT;TWABS;USTXT;VEN;EPTXT;WOTXT:区块链, 授权, 智能合约, 智能合同, 令牌, 节点, 数据, 交易, 加密, block chain, blockchain, authorization, smart contract, token, node, data, transaction, 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
PX	CN 110457875 A (阿里巴巴集团控股有限公司) 2019年 11月 15日 (2019 - 11 - 15) 全文	1-20
X	WO 2019078879 A1 (HEWLETT PACKARD ENTPR DEV LP) 2019年 4月 25日 (2019 - 04 - 25) 说明书第10-70段, 附图1-5	1-20
A	CN 110011996 A (阿里巴巴集团控股有限公司) 2019年 7月 12日 (2019 - 07 - 12) 全文	1-20
A	CN 109639643 A (平安科技深圳有限公司) 2019年 4月 16日 (2019 - 04 - 16) 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

2020年 4月 27日

国际检索报告邮寄日期

2020年 5月 8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

杨牛

电话号码 86-(20)-28950388

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2020/072153

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	110457875	A	2019年 11月 15日	无	
W0	2019078879	A1	2019年 4月 25日	无	
CN	110011996	A	2019年 7月 12日	无	
CN	109639643	A	2019年 4月 16日	无	