

(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



(10) 国际公布号

(43) 国际公布日
2020 年 12 月 30 日 (30.12.2020)

WIPO PCT

WO 2020/258941 A1

- (51) 国际专利分类号:
H04L 29/06 (2006.01) **H04L 9/32** (2006.01)
- (21) 国际申请号: PCT/CN2020/080734
- (22) 国际申请日: 2020 年 3 月 23 日 (23.03.2020)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201910575178.1 2019年6月28日 (28.06.2019) CN
- (71) 申请人: 华为技术有限公司 (HUAWEI TECHNOLOGIES CO., LTD.) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

- (72) 发明人: 侯庆辉(HOU, Qinghui); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 潘瑜(PAN, Yu); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 胡瑞丰(HU, Ruifeng); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。
- (74) 代理人: 北京润泽恒知识产权代理有限公司 (BEIJING RUN ZEHENG INTELLECTUAL PROPERTY LAW FIRM); 中国北京市海淀区中关村南大街 31 号神舟大厦 702, Beijing 100081 (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,

(54) Title: METHOD FOR DATA OWNERSHIP CONFIRMATION BASED ON BLOCKCHAIN NETWORK, AND RELATED APPARATUS

(54) 发明名称: 基于区块链网络的数据确权方法及相关装置

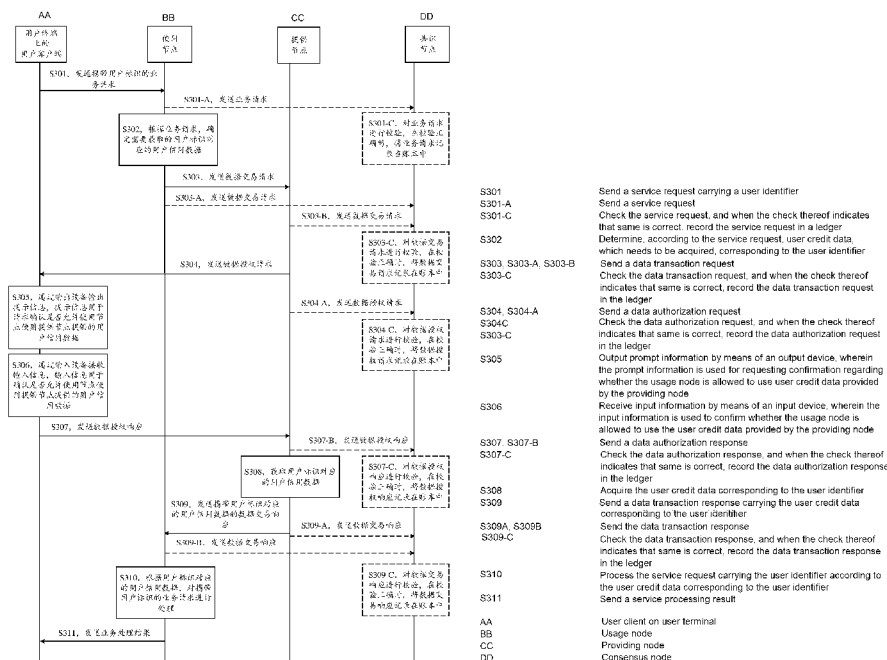


图 3

(57) Abstract: A method, apparatus and system for data ownership confirmation based on a blockchain network. The method comprises: a first blockchain node in a blockchain network sending or receiving communication information; and recording the communication information in a ledger, wherein the blockchain network comprises a usage node and a providing node, the usage node is used for requesting user credit data according to a service request, and the providing node is used for providing the user credit data; and the communication information comprises information between the first blockchain node and another blockchain node or a user client.

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: 一种基于区块链网络的数据确权方法、装置及系统, 方法包括: 区块链网络中的第一区块链节点发送或者接收通信信息; 将通信信息记录在账本中; 区块链网络包括使用节点和提供节点; 使用节点, 用于根据业务请求请求用户信用数据; 提供节点, 用于提供用户信用数据; 通信信息包括: 第一区块链节点与其他区块链节点或者用户客户端之间的信息。

基于区块链网络的数据确权方法及相关装置

本申请要求于 2019 年 06 月 28 日提交中国专利局、申请号为 201910575178.1、申请名称为“基于区块链网络的数据确权方法及相关装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请涉及区块链领域技术，尤其涉及基于区块链网络的数据确权方法及相关装置。

背景技术

随着信息技术的发展，人们的日常生活与数字世界的结合越来越紧密。当用户在日常生活中需要向一些业务服务的提供商申请业务服务时，业务服务的提供商需要对用户的个人信息进行检验，以确定是否向用户提供该用户所申请的业务服务。例如，银行可以向用户提供各种类型的金融服务，银行在受理用户的业务请求后，需要向第三方数据提供商获取可信的用户数据，以便根据获取到的用户数据确认是否向用户提供相应服务。第三方数据提供商可以预先记录海量用户的用户数据。

在这一类业务处理的场景中，使用数据的机构可以称为数据使用商，提供数据的第三方数据提供商可以称为数据提供商，在开始接收业务请求之前，数据使用商可以预先与数据提供商签订数据交易合约，约定允许数据使用商获取并使用的数据等，这样，数据使用商在接收到用户的业务请求后，可以随时从数据使用商获取需要的用户数据，并对用户申请的业务进行处理。

但是，采用这种处理方式，由于数据使用商与数据提供商之间交易用户数据的过程信息，仅仅记录在数据使用商和数据提供商的服务器上，当用户怀疑自身的用户数据泄露时，仅仅通过数据使用商和数据提供商两方记录的过程信息，无法确定数据是由哪一方泄露的。

为了提高用户数据的安全性，目前，亟需一种可追溯的数据使用的方法。

发明内容

本申请提供了一种基于区块链网络的数据确权方法及相关装置，能够提供一种可追溯的数据使用方法来提高用户数据的安全性。

第一方面，本申请提供一种基于区块链网络的数据确权方法，所述方法包括：

区块链网络中的第一区块链节点发送或者接收通信信息；

所述第一区块链节点将所述通信信息记录在区块链网络的账本中；

其中，所述区块链网络包括多个区块链节点，所述多个区块链节点包括：使用节点和提供节点；所述使用节点，用于根据携带有用户标识的业务请求，向所述提供节点请求所述用户标识对应的用户信用数据；所述提供节点，用于向所述使用节点提供用户信用数据；所述通信信息包括：所述第一区块链节点与所述多个区块链节点中的任一其他区块链节点之间的信息，以及，第一区块链节点与用户客户端之间的信息中至少一种；其中，所述用户客户端用于向所述使用节点发送携带有所述用户标识的所述业务请求，和/或，所述用

户客户端用于确认是否允许所述提供节点向所述使用节点提供所述用户标识对应的用户信用数据；所述第一区块链节点为所述多个区块链节点中的区块链节点。

在本申请中，当采用区块链网络部署数据使用场景中的使用节点和提供节点，并利用区块链网络中的账本记录区块链节点之间以及区块链节点与用户客户端之间的通信信息，
5 能够实现一种可追溯的数据使用方法。

示例性地，第一区块链节点并不特指区块链节点中的具有特定编号的区块链节点，在本申请实施例中，第一区块链节点可以是区块链网络的多个区块链节点中的使用节点、提供节点、代理节点中任一种或多种区块链节点。本申请实施例提供的技术方案能够将使用节点、提供节点、代理节点间交互的通信信息以及使用节点和提供节点与用户终端上的用户客户端交互的通信信息记录在区块链的账本中，来实现数据使用的可追溯的需求。
10

在一种可能的实现方式中，所述区块链网络还包括：共识节点；所述第一区块链节点为所述多个区块链节点中除所述共识节点之外的区块链节点；

所述第一区块链节点将所述通信信息记录在区块链网络的账本中，包括：

所述第一区块链节点向所述共识节点发送所述通信信息，以使所述共识节点将所述通信信息以区块的形式发送给区块链网络中的记账节点，所述记账节点用于将包含所述通信信息的区块记录在区块链网络的账本中。举例来说，记账节点为所述区块链网络中除所述共识节点之外的区块链节点，示例性地，记账节点可以为使用节点、提供节点等区块链节点。
15

在一种可能的实现方式中，所述区块链网络中的第一区块链节点发送或者接收通信信息，包括：
20

所述第一区块链节点向第二区块链节点发送所述通信信息；或者，

所述第一区块链节点接收所述第二区块链节点发送的所述通信信息；或者，

所述第一区块链节点向所述用户客户端发送所述通信信息；或者，

所述第一区块链节点接收所述用户客户端发送的所述通信信息；
25

其中，所述第二区块链节点为所述多个区块链节点中除所述第一区块链节点之外的任一其他区块链节点。

在一种可能的实现方式中，所述第一区块链节点为所述使用节点；所述用户客户端用于向所述使用节点发送携带有所述用户标识的所述业务请求；

所述区块链网络中的第一区块链节点发送或者接收通信信息，包括：所述使用节点发送或者接收通信信息，其中，所述通信信息具体包括：所述使用节点与所述多个区块链节点中的其他区块链节点之间的信息，以及，所述使用节点与所述用户客户端之间的信息中至少一种。示例性地，使用节点可以在发送或者接收通信信息之后，向共识节点发送通信信息，所述共识节点为所述多个区块链节点中除所述使用节点之外的任一区块链节点。
30

在一种可能的实现方式中，所述第一区块链节点为所述提供节点；所述用户客户端用于确认是否允许所述提供节点向所述使用节点提供所述用户标识对应的用户信用数据；
35

所述区块链网络中的第一区块链节点发送或者接收通信信息，包括：所述提供节点发送或者接收通信信息，其中，所述通信信息具体包括：所述提供节点与所述多个区块链节点中的其他区块链节点之间的信息，以及，所述提供节点与所述用户客户端之间的信息中至少一种；所述共识节点为所述多个区块链节点中除所述提供节点之外的任一区块链节点

点。

在一种可能的实现方式中，所述第一区块链节点为所述使用节点；所述区块链网络中的第一区块链节点发送或者接收通信信息，包括以下至少一种：

所述使用节点接收所述用户客户端发送的业务请求；

- 5 所述使用节点向所述提供节点发送数据交易请求，所述数据交易请求用于请求获取所述用户标识对应的用户信用数据，所述用户信用数据用于所述使用节点处理携带有所述用户标识的业务请求；

所述使用节点接收所述提供节点发送的数据交易响应，所述数据交易响应包括所述用户标识对应的用户信用数据。

- 10 相应的，上述通信信息可以具体包括以下至少一种：

所述使用节点接收到的由所述用户客户端发送的携带所述用户标识的业务请求；

所述使用节点向所述提供节点发送的数据交易请求，所述数据交易请求用于请求获取所述用户标识对应的用户信用数据，所述用户信用数据用于所述使用节点处理携带有所述用户标识的业务请求；

- 15 所述使用节点从所述提供节点接收的数据交易响应，所述数据交易响应包括所述用户标识对应的用户信用数据。

在一种可能的实现方式中，所述第一区块链节点为所述提供节点；所述区块链网络中的第一区块链节点发送或者接收通信信息，包括以下至少一种：

- 20 所述提供节点接收所述使用节点发送的数据交易请求，所述数据交易请求用于请求获取所述用户标识对应的用户信用数据，所述用户信用数据用于所述使用节点处理携带有所述用户标识的业务请求；

所述提供节点向所述用户客户端发送数据授权请求，所述数据授权请求用于请求允许向所述使用节点提供所述用户标识对应的用户信用数据；

- 25 所述提供节点接收所述用户客户端发送的数据授权响应，所述数据授权响应用于确认是否允许向所述使用节点提供所述用户标识对应的用户信用数据；

所述提供节点向所述使用节点发送数据交易响应，所述数据交易响应包括所述用户标识对应的用户信用数据。

相应地，所述通信信息具体包括以下至少一种：

- 30 所述提供节点从所述使用节点接收到的数据交易请求，所述数据交易请求用于请求获取所述用户标识对应的用户信用数据，所述用户信用数据用于所述使用节点处理携带有所述用户标识的业务请求；

所述提供节点向所述用户客户端发送的数据授权请求，所述数据授权请求用于确认是否允许向所述使用节点提供所述用户标识对应的用户信用数据；

- 35 所述提供节点从所述用户客户端接收的数据授权响应，所述数据授权响应包括所述用户标识对应的用户信用数据；

所述提供节点向所述使用节点发送的数据交易响应，所述数据交易响应包括所述用户标识对应的用户信用数据。

在一种可能的实现方式中，所述多个区块链节点包括：代理节点；所述代理节点，用于接收所述使用节点发送的数据交易请求，所述数据交易请求用于请求所述用户标识对应

的用户信用数据；以及，确认所述使用节点是否具有所述用户标识对应的用户信用数据的访问权限；以及，在确认所述使用节点具有访问权限时，向所述提供节点发送所述数据交易请求；以及，接收所述提供节点发送的数据交易响应，所述数据交易响应包括所述用户标识对应的用户信用数据；

5 所述第一区块链节点为所述代理节点；所述区块链网络中的第一区块链节点发送或者接收通信信息，包括：所述代理节点发送或者接收通信信息，其中，所述通信信息具体包括：所述代理节点与所述使用节点之间的信息，所述代理节点与所述提供节点之间的信息中至少一种；所述共识节点为所述多个区块链节点中除所述代理节点之外的任一区块链节点。

10 在一种可能的实现方式中，所述区块链网络包括：X个通道；所述区块链网络中的区块链节点分别对应X个通道中的一个或多个通道；其中，所述第一区块链节点对应的通道包括第i通道，所述区块链网络中的第二区块链节点对应的通道包括第i通道；

 所述第一区块链节点将所述通信信息记录在区块链网络的账本中，包括：所述第一区块链节点将所述第i通道的通道信息记录在第i通道对应的账本中；

15 所述第i通道的通道信息包括：所述第一区块链节点与所述第二区块链节点之间通过第i通道传输的信息，以及，所述第一区块链节点或者所述第二区块链节点基于从所述第i通道接收的信息向所述用户客户端发送的信息，以及，所述第一区块链节点基于从所述用户客户端接收的信息通过第i通道向第二区块链节点发送的信息，以及，所述第二区块链节点基于从所述用户客户端接收的信息通过第i通道向所述第一区块链节点发送的信息
20 中至少一种；其中，X为大于0的整数，i为大于0且小于或者等于X的整数。

 示例性地，第一区块链节点可以通过所述第i通道向区块链网络中的共识节点发送第i通道的通道信息，以使共识节点对第i通道的通信信息进行打包，生成区块，并将区块发送给所属通道为第i通道的记账节点，第i通道的记账节点可用于将第i通道的通道信息记录在第i通道的账本中。

25 在一种可能的实现方式中，所述区块链网络包括M个使用节点，M个使用节点分别对应X个通道中的一个通道，任一使用节点通过自身对应的通道与提供节点传输信息；所述共识节点对应一个或多个通道；

 所述第一区块链节点为M个使用节点中对应的通道为第i通道的第j个使用节点，所述第二区块链节点为通过第i通道与第j个使用节点传输信息的提供节点；或者，所述第一区块链节点为与对应的通道为第i通道的第j个使用节点通过第i通道传输信息的提供节点，所述第二区块链节点为第j个使用节点；
30 其中，M为大于0的整数，j为大于0且小于或者等于M的整数。

 在一种可能的实现方式中，所述区块链网络包括M个使用节点，M个使用节点分别对应X个通道中的一个通道，任一使用节点通过自身对应的通道与提供节点传输信息；

35 所述多个区块链节点包括：代理节点；所述代理节点，用于接收所述使用节点发送的数据交易请求，所述数据交易请求用于请求所述用户标识对应的用户信用数据；以及，确认所述使用节点是否具有所述用户标识对应的用户信用数据的访问权限；以及，在确认所述使用节点具有访问权限时，向所述提供节点发送所述数据交易请求；以及，接收所述提供节点发送的数据交易响应，所述数据交易响应包括所述用户标识对应的用户信用数据；

所述第一区块链节点为 M 个使用节点中对应的通道为第 i 通道的第 j 个使用节点，所述第二区块链节点为与第 j 个使用节点通过第 i 通道传输信息的代理节点；或者，所述第一区块链节点为与对应的通道为第 i 通道的第 j 个使用节点通过第 i 通道传输信息的代理节点，所述第二区块链节点为第 j 个使用节点；或者，所述第一区块链节点为与对应的通道为第 i 通道的第 j 个使用节点通过第 i 通道传输信息的代理节点，所述第二区块链节点为与所述第一区块链节点通过第 i 通道传输信息的提供节点；

其中， M 为大于 0 的整数， j 为大于 0 且小于或者等于 M 的整数。

示例性地，区块链网络中的共识节点可以对应一个或多个通道。

在一种可能的实现方式中，所述提供节点为运营商服务器；所述用户信用数据为所述用户标识对应的运营商信用数据。

第二方面，本申请提供一种基于区块链网络的数据确权方法，所述方法包括：

共识节点接收通信信息，并将所述通信信息记录在区块链网络的账本中；

其中，所述区块链网络包括多个区块链节点，所述多个区块链节点包括：使用节点和提供节点；所述使用节点，用于根据携带有用户标识的业务请求，向所述提供节点请求所述用户标识对应的用户信用数据；所述提供节点，用于向所述使用节点提供用户信用数据；所述共识节点为所述多个区块链节点中的区块链节点；所述通信信息包括：区块链节点之间的信息，以及，区块链节点与用户客户端之间的信息中至少一种；其中，所述用户客户端用于向所述使用节点发送携带有所述用户标识的所述业务请求，和/或，所述用户客户端用于确认是否允许所述提供节点向所述使用节点提供所述用户标识对应的用户信用数据。

示例性地，共识节点可以从第一方面所述方法中的第一区块链节点接收通信信息。第一区块链节点可以为区块链网络的多个区块链节点中的使用节点、提供节点、代理节点。

在一种可能的实现方式中，所述通信信息包括所述通信信息的发送方；

所述将所述通信信息记录在区块链网络的账本中，包括：

所述共识节点对所述通信信息的发送方进行校验；

在校验成功时，共识节点可以将所述通信信息封装为区块，发送给记账节点，以使所述记账节点将所述通信信息记录在所述记账节点本地存储的账本中；

其中，区块链网络中的记账节点为区块链网络中本地存储有账本或者账本副本的区块链节点。示例性地，记账节点可以是第一方面中的第一区块链节点。

在一种可能的实现方式中，所述通信信息包括：所述使用节点与所述多个区块链节点中的其他区块链节点之间的信息，以及，所述使用节点与所述用户客户端之间的信息中至少一种；所述用户客户端用于向所述使用节点发送携带有所述用户标识的所述业务请求；

所述共识节点为所述多个区块链节点中除所述使用节点之外的任一区块链节点；

所述共识节点接收通信信息，包括：所述共识节点接收所述使用节点发送的所述通信信息。

在一种可能的实现方式中，所述通信信息包括：所述提供节点与所述多个区块链节点中的其他区块链节点之间的信息，以及，所述提供节点与所述用户客户端之间的信息中至少一种；所述用户客户端用于确认是否允许所述提供节点向所述使用节点提供所述用户标识对应的用户信用数据；

所述共识节点为所述多个区块链节点中除所述提供节点之外的任一区块链节点；

所述共识节点接收通信信息，包括：所述共识节点接收所述提供节点发送的所述通信信息。

在一种可能的实现方式中，所述区块链网络还包括：代理节点；所述代理节点，用于接收所述使用节点发送的数据交易请求，所述数据交易请求用于请求所述用户标识对应的用户信用数据；以及，确认所述使用节点是否具有所述用户标识对应的用户信用数据的访问权限；以及，在确认所述使用节点具有访问权限时，向所述提供节点发送所述数据交易请求；以及，接收所述提供节点发送的数据交易响应，所述数据交易响应包括所述用户标识对应的用户信用数据；

所述共识节点接收通信信息，包括：所述共识节点接收所述代理节点发送的所述通信信息；其中，所述通信信息具体包括：所述代理节点与所述使用节点之间的信息，所述代理节点与所述提供节点之间的信息中至少一种。

在一种可能的实现方式中，所述区块链网络包括：X个通道；所述区块链网络中的区块链节点分别对应X个通道中的一个或多个通道；其中，所述使用节点的数量为M个，M个使用节点分别对应X个通道中的一个通道，任一使用节点通过自身对应的通道与提供节点传输信息；所述共识节点对应一个或多个通道；

所述共识节点接收通信信息包括：所述共识节点接收所述共识节点对应的第i通道的通道信息，并将接收到的所述第i通道的通道信息打包为区块，发送给所属通道为第i通道的记账节点，以使该记账节点将第i通道的通信信息记录在第i通道对应的账本中；

第i通道的通道信息包括以下至少一种：

对应的通道为第i通道的使用节点与第一用户客户端之间的信息，所述第一用户客户端用于向所述使用节点发送携带有所述用户标识的所述业务请求；

对应的通道为第i通道的使用节点与提供节点之间的信息，

提供节点基于从第i通道接收的信息向第二用户客户端发送的信息以及从用户终端接收的信息；所述第二用户客户端用于确认是否允许所述提供节点向所述使用节点提供所述用户标识对应的用户信用数据；

其中，X为大于0的整数，M为大于0的整数，i为大于0且小于或者等于X的整数。

第三方面，本申请提供一种基于区块链网络的数据确权方法，所述方法包括：

用户客户端接收提供节点发送的携带有所述用户客户端对应的用户标识的数据授权请求，所述数据授权请求用于请求允许使用节点使用所述提供节点提供的所述用户标识对应的用户信用数据；

所述用户客户端通过输出设备输出提示信息，所述提示信息用于请求确认是否允许所述使用节点使用所述提供节点提供的所述用户标识对应的用户信用数据；

其中，所述使用节点、所述提供节点为区块链网络中的区块链节点，所述使用节点用于向所述提供节点请求用户标识对应的用户信用数据。

在本申请中，当采用区块链网络部署数据使用场景中的使用节点和提供节点，并利用区块链网络中的提供节点向用户客户端请求确认是否允许使用节点使用提供节点所提供的用户标识对应的用户信用数据，用户可以及时了解数据的使用情况，因此，本申请能够实现一种可追溯的数据使用方法。

在本申请中，用户终端上可以部署用户客户端（如第二用户客户端），该用户客户端可以用于与一个或多个提供节点通信，例如，接收一个或多个提供节点发送的数据授权请求，以及，向一个或多个提供节点发送数据授权响应。该用户客户端可以将来自多个提供节点的数据授权请求整合后通过输出设备输出提示信息。该用户客户端可以对应一个用户标识，从而可以使得用户可以对来自一个或多个提供节点的一个或多个用户信用数据的数据授权请求进行集中确认。在一些情况下，该用户客户端还可以用于与一个或多个使用节点通信（即该用户客户端可以同时具有第一用户客户端的功能，第一用户客户端与第二用户客户端对应相同的用户标识），例如，向一个或多个使用节点发送业务请求，以及，接收一个或多个使用节点发送的业务处理结果。

在一种可能的实现方式中，用户客户端接收提供节点发送的数据授权请求，可以包括：用户客户端接收提供节点发送的数据授权请求，所述数据授权请求包括数据源列表和用户标识对应的用户信用数据的标识列表，其中，数据源列表包括一个或多个提供节点的标识。在一种实施方式中，提供节点发送的数据授权请求可以为第二数据授权请求，提供节点可以在接收到代理节点发送的第一数据授权请求后发送第二数据授权请求，需要说明的是，使用节点向代理节点发送数据交易请求时，可以包括数据源列表和用户信用数据的标识的列表，代理节点可以分别向数据源列表中的多个提供节点发送第一数据授权请求，任一第一数据授权请求可以包含数据源列表和用户信用数据的标识列表。

在一种可能的实现方式中，所述用户客户端接收提供节点发送的携带有所述用户客户端对应的用户标识的数据授权请求，包括：所述用户客户端接收至少两个提供节点发送的至少两个数据授权请求，所述至少两个数据授权请求分别与所述至少两个提供节点一一对应，任一数据授权请求用于请求所述用户客户端允许所述使用节点使用发送数据授权请求的提供节点提供的用户标识对应的用户信用数据；

其中，所述使用节点用于分别向所述至少两个提供节点请求所述用户标识对应的用户信用数据，所述用户标识对应的用户信用数据包括：由所述至少两个提供节点分别提供的所述用户标识对应的用户信用数据；

所述提示信息用于请求确认是否允许所述使用节点使用所述至少两个提供节点分别提供的所述用户标识对应的用户信用数据。

在一种可能的实现方式中，所述方法还包括：

所述用户客户端通过自身的输出设备输出提示信息，所述提示信息用于请求确认是否允许所述使用节点使用所述至少两个提供节点分别提供的所述用户标识对应的用户信用数据；

所述用户客户端通过输入设备接收输入信息，所述输入信息用于确认是否允许所述使用节点使用所述至少两个提供节点所提供的所述用户标识对应的用户信用数据；

在所述输入信息表示允许所述使用节点使用所述至少两个提供节点所提供的所述用户标识对应的用户信用数据时，所述用户终端分别向所述提供节点发送数据授权响应，任一所述数据授权响应用于确认允许所述使用节点使用接收数据授权响应的提供节点所提供的所述用户标识对应的用户信用数据。

在一种可能的实现方式中，所述数据授权请求用于请求允许所述使用节点在接收到第一业务的业务请求时，使用所述提供节点所提供的所述用户标识对应的用户信用数据。

第四方面，本申请提供一种基于区块链网络的数据确权系统，所述系统包括：多个区块链节点；所述多个区块链节点包括：使用节点和提供节点；其中，所述使用节点，用于根据携带有用户标识的业务请求，向所述提供节点请求所述用户标识对应的用户信用数据；所述提供节点，用于提供用户信用数据；

5 所述多个区块链节点中的至少一个区块链节点，还用于发送或者接收通信信息，并将所述通信信息记录在区块链网络的账本中；其中，所述通信信息包括：区块链节点之间的信息，以及，区块链节点与用户客户端之间的信息中至少一种；其中，所述用户客户端用于向所述使用节点发送携带有所述用户标识的所述业务请求，和/或，所述用户客户端用于确认是否允许所述提供节点向所述使用节点提供所述用户标识对应的用户信用数据。

10 在本申请实施例中，上述至少一个区块链节点可以将通信信息发送给区块链网络中的共识节点，共识节点对通信信息进行打包，生成区块，并发送给记账节点，记账节点可以将包含通信信息的区块存储在区块链网络的账本中。示例性地，共识节点可以是除了使用节点或者提供节点或者代理节点之外的区块链节点。

15 在一种可能的实现方式中，所述至少一个区块链节点为使用节点；所述通信信息具体包括：所述使用节点与所述多个区块链节点中的其他区块链节点之间的信息，以及，所述使用节点与所述用户客户端之间的信息中至少一种；所述用户客户端用于向所述使用节点发送携带有所述用户标识的所述业务请求。

20 示例性地，所述使用节点，还可以用于在发送或者接收所述通信信息后，向所述共识节点发送所述通信信息；共识节点可以为所述多个区块链节点中除所述使用节点之外的任一区块链节点。

在一种可能的实现方式中，所述通信信息具体包括以下至少一种：

所述使用节点接收到的所述用户客户端发送的携带所述用户标识的业务请求；

25 所述使用节点向所述提供节点发送的数据交易请求，所述数据交易请求用于请求获取所述用户标识对应的用户信用数据，所述用户信用数据用于所述使用节点处理携带有所述用户标识的业务请求；

所述使用节点从所述提供节点接收的数据交易响应，所述数据交易响应包括所述用户标识对应的用户信用数据。

在一种可能的实现方式中，所述至少一个区块链节点为提供节点；

30 所述通信信息具体包括：所述提供节点与所述多个区块链节点中的其他区块链节点之间的信息，以及，所述提供节点与所述用户客户端之间的信息中至少一种；所述用户客户端用于确认是否允许所述提供节点向所述使用节点提供所述用户标识对应的用户信用数据。

35 示例性地，所述提供节点，还用于在发送或者接收所述通信信息后，向共识节点发送所述通信信息；所述共识节点为所述至少两个区块链节点中除所述提供节点之外的任一区块链节点。

在一种可能的实现方式中，所述通信信息具体包括以下至少一种：

所述提供节点从所述使用节点接收到的数据交易请求，所述数据交易请求用于请求获取所述用户标识对应的用户信用数据，所述用户标识对应的用户信用数据用于所述使用节点处理携带有所述用户标识的业务请求；

所述提供节点向所述用户客户端发送的数据授权请求,所述数据授权请求用于请求允许所述使用节点使用所述提供节点所提供的所述用户标识对应的用户信用数据;

所述提供节点从所述用户客户端接收的数据授权响应,所述数据授权响应包括所述用户标识对应的用户信用数据;

5 所述提供节点向所述使用节点发送的数据交易响应,所述数据交易响应包括所述用户标识对应的用户信用数据。

在一种可能的实现方式中,所述多个区块链节点还包括:代理节点;

所述代理节点,用于接收所述使用节点发送的数据交易请求,所述数据交易请求用于请求所述用户标识对应的用户信用数据;以及,确认所述使用节点是否具有所述用户标识对应的用户信用数据的访问权限;以及,在确认所述使用节点具有访问权限时,向所述提供节点发送所述数据交易请求;以及,接收所述提供节点发送的数据交易响应,所述数据交易响应包括所述用户标识对应的用户信用数据;

所述通信信息具体包括:所述代理节点与所述使用节点之间的信息,所述代理节点与所述提供节点之间的信息中至少一种。

15 在一种可能的实现方式中,所述区块链网络包括:X个通道;所述多个区块链节点分别对应X个通道中的一个或多个通道;其中,

所述使用节点的数量为M个,M个使用节点分别对应X个通道中的一个通道,任一使用节点通过自身对应的通道与提供节点传输信息;

第i通道的通道信息包括以下至少一种:

20 对应的通道为第i通道的使用节点与第一用户客户端之间的信息,所述第一用户客户端用于向所述使用节点发送携带有所述用户标识的所述业务请求;

对应的通道为第i通道的使用节点与提供节点之间的信息;

提供节点基于从第i通道接收的信息向第二用户客户端发送的信息以及从第二用户客户端接收的信息;所述第二用户客户端用于确认是否允许所述提供节点向所述使用节点提供所述用户标识对应的用户信用数据;

其中,X为大于0的整数,M为大于0的整数,i为大于0且小于或者等于X的整数。

30 示例性地,区块链网络中共识节点的数量为Y个,任一共识节点对应一个或多个通道,所述Y个共识节点中的第j个共识节点,具体用于接收第j个共识节点对应的第i通道的通道信息,并将接收到的第i通道的通道信息记录在第i通道对应的账本中;Y为大于0的整数,j为大于0且小于或者等于Y的整数。

在本申请中,区块链网络中的任一区块链节点可以通过在对应的通道内广播的方式向对应通道相同的其他区块链节点发送信息。

35 在一种可能的实现方式中,所述提供节点,还用于向所述用户客户端发送数据授权请求,所述数据授权请求用于请求允许所述使用节点使用所述提供节点提供的所述用户标识对应的用户信用数据。

在一种可能的实现方式中,所述提供节点为运营商服务器;所述用户信用数据为所述用户标识对应的运营商信用数据。

第五方面,本申请还提供一种基于区块链网络的数据确权装置,应用于区块链网络中的第一区块链节点,所述装置包括:

收发模块，用于发送或者接收通信信息；

处理模块，用于将所述通信信息记录在区块链网络的账本中；

其中，所述区块链网络包括多个区块链节点，所述多个区块链节点包括：使用节点和提供节点；所述使用节点，用于根据携带有用户标识的业务请求，向所述提供节点请求所述用户标识对应的用户信用数据；所述提供节点，用于向所述使用节点提供用户信用数据；所述通信信息包括：所述第一区块链节点与所述多个区块链节点中的任一其他区块链节点之间的信息，以及，第一区块链节点与用户客户端之间的信息中至少一种；其中，所述用户客户端用于向所述使用节点发送携带有所述用户标识的所述业务请求，和/或，所述用户客户端用于确认是否允许所述提供节点向所述使用节点提供所述用户标识对应的用户信用数据；所述第一区块链节点为所述多个区块链节点中的区块链节点。

示例性地，所述收发模块，还用于向共识节点发送所述通信信息，以使所述共识节点将所述通信信息记录在区块链网络的账本中；所述共识节点为所述多个区块链节点中除所述第一区块链节点之外的区块链节点；

在一种可能的实现方式中，所述收发模块，具体用于：

向第二区块链节点发送所述通信信息；或者，
接收所述第二区块链节点发送的所述通信信息；或者，
向所述用户客户端发送所述通信信息；或者，
接收所述用户客户端发送的所述通信信息；

其中，所述第二区块链节点为所述多个区块链节点中除所述第一区块链节点之外的任一其他区块链节点。

在一种可能的实现方式中，所述第一区块链节点为所述使用节点；所述用户客户端用于向所述使用节点发送携带有所述用户标识的所述业务请求；

所述收发模块，具体用于发送或者接收通信信息，其中，所述通信信息具体包括：所述使用节点与所述多个区块链节点中的其他区块链节点之间的信息，以及，所述使用节点与所述用户客户端之间的信息中至少一种；所述共识节点为所述多个区块链节点中除所述使用节点之外的任一区块链节点。

在一种可能的实现方式中，所述第一区块链节点为所述提供节点；所述用户客户端用于确认是否允许所述提供节点向所述使用节点提供所述用户标识对应的用户信用数据；

所述收发模块，具体用于发送或者接收通信信息，其中，所述通信信息具体包括：所述提供节点与所述多个区块链节点中的其他区块链节点之间的信息，以及，所述提供节点与所述用户客户端之间的信息中至少一种；所述共识节点为所述多个区块链节点中除所述提供节点之外的任一区块链节点。

在一种可能的实现方式中，所述第一区块链节点为所述使用节点；所述用户客户端用于向所述使用节点发送携带有所述用户标识的所述业务请求；所述收发模块，具体用于以下至少一种：

接收所述用户客户端发送的携带有所述用户标识的所述业务请求；

向所述提供节点发送数据交易请求，所述数据交易请求用于请求获取所述用户标识对应的用户信用数据，所述用户信用数据用于所述使用节点处理携带有所述用户标识的业务请求；

接收所述提供节点发送的数据交易响应,所述数据交易响应包括所述用户标识对应的用户信用数据。

在一种可能的实现方式中,所述第一区块链节点为所述提供节点;所述用户客户端用于确认是否允许所述提供节点向所述使用节点提供所述用户标识对应的用户信用数据;所述收发模块,具体用于以下至少一种:

接收所述使用节点发送的数据交易请求,所述数据交易请求用于请求获取所述用户标识对应的用户信用数据,所述用户信用数据用于所述使用节点处理携带有所述用户标识的业务请求;

向所述用户客户端发送数据授权请求,所述数据授权请求用于请求所述用户客户端允许向所述使用节点提供所述用户标识对应的用户信用数据;

接收所述用户客户端发送的数据授权响应,所述数据授权响应用于确认是否允许向所述使用节点提供所述用户标识对应的用户信用数据;

向所述使用节点发送数据交易响应,所述数据交易响应包括所述用户标识对应的用户信用数据。

在一种可能的实现方式中,所述多个区块链节点包括:代理节点;所述代理节点,用于接收所述使用节点发送的数据交易请求,所述数据交易请求用于请求所述用户标识对应的用户信用数据;以及,确认所述使用节点是否具有所述用户标识对应的用户信用数据的访问权限;以及,在确认所述使用节点具有访问权限时,向所述提供节点发送所述数据交易请求;以及,接收所述提供节点发送的数据交易响应,所述数据交易响应包括所述用户标识对应的用户信用数据;

所述第一区块链节点为所述代理节点;所述收发模块,具体用于发送或者接收通信信息,其中,所述通信信息具体包括:所述代理节点与所述使用节点之间的信息,所述代理节点与所述提供节点之间的信息中至少一种。

示例性地,所述收发模块可以在发送或者接收通信信息后向共识节点发送通信信息,所述共识节点为所述多个区块链节点中除所述代理节点之外的任一区块链节点。

在一种可能的实现方式中,所述区块链网络包括:X个通道;所述区块链网络中的区块链节点分别对应X个通道中的一个或多个通道;其中,所述第一区块链节点对应的通道包括第i通道,所述区块链网络中的第二区块链节点对应的通道包括第i通道;

所述收发模块,具体用于将所述第i通道的通道信息记录在第i通道对应的账本中;

所述第i通道的通道信息包括:所述第一区块链节点与所述第二区块链节点之间通过第i通道传输的信息,以及,所述第一区块链节点或者所述第二区块链节点基于从所述第i通道接收的信息向所述用户客户端发送的信息,以及,所述第一区块链节点基于从所述用户客户端接收的信息通过第i通道向第二区块链节点发送的信息,以及,所述第二区块链节点基于从所述用户客户端接收的信息通过第i通道向所述第一区块链节点发送的信息中至少一种;

其中,X为大于0的整数,i为大于0且小于或者等于X的整数。

示例性地,收发模块可以通过所述第i通道向所述共识节点发送第i通道的通道信息,以使所述共识节点打包第i通道的通信信息,生成区块,并将区块发送给第i通道对应的记账节点,第i通道的记账节点将第i通道的通信信息记录在第i通道对应的账本中。

在一种可能的实现方式中，所述区块链网络包括M个使用节点，M个使用节点分别对应X个通道中的一个通道，任一使用节点通过自身对应的通道与提供节点传输信息；所述共识节点对应一个或多个通道；

5 所述第一区块链节点为M个使用节点中对应的通道为第i通道的第j个使用节点，所述第二区块链节点为通过第i通道与第j个使用节点传输信息的提供节点；或者，所述第一区块链节点为与对应的通道为第i通道的第j个使用节点通过第i通道传输信息的提供节点，所述第二区块链节点为第j个使用节点；

其中，M为大于0的整数，j为大于0且小于或者等于M的整数。

10 在一种可能的实现方式中，所述区块链网络包括M个使用节点，M个使用节点分别对应X个通道中的一个通道，任一使用节点通过自身对应的通道与提供节点传输信息；

所述多个区块链节点包括：代理节点；所述代理节点，用于接收所述使用节点发送的数据交易请求，所述数据交易请求用于请求所述用户标识对应的用户信用数据；以及，确认所述使用节点是否具有所述用户标识对应的用户信用数据的访问权限；以及，在确认所述使用节点具有访问权限时，向所述提供节点发送所述数据交易请求；以及，接收所述提供节点发送的数据交易响应，所述数据交易响应包括所述用户标识对应的用户信用数据；

15 所述第一区块链节点为M个使用节点中对应的通道为第i通道的第j个使用节点，所述第二区块链节点为与第j个使用节点通过第i通道传输信息的代理节点；或者，所述第一区块链节点为与对应的通道为第i通道的第j个使用节点通过第i通道传输信息的代理节点，所述第二区块链节点为第j个使用节点；或者，所述第一区块链节点为与对应的通道为第i通道的第j个使用节点通过第i通道传输信息的代理节点，所述第二区块链节点为与所述第一区块链节点通过第i通道传输信息的提供节点；其中，M为大于0的整数，j为大于0且小于或者等于M的整数。

示例性地，区块链网络中的共识节点对应一个或多个通道。

25 在一种可能的实现方式中，所述提供节点为运营商服务器；所述用户信用数据为所述用户标识对应的运营商信用数据。

第六方面，本申请还提供一种基于区块链网络的数据确权装置，应用于用户客户端，所述装置包括：

30 收发模块，用于接收提供节点发送的携带有所述用户客户端对应的用户标识的数据授权请求，所述数据授权请求用于请求允许使用节点使用所述提供节点提供的所述用户标识对应的用户信用数据；

输出模块，用于通过输出设备输出提示信息，所述提示信息用于请求确认是否允许所述使用节点使用所述提供节点提供的所述用户标识对应的用户信用数据；

其中，所述使用节点、所述提供节点为区块链网络中的区块链节点，所述使用节点用于向所述提供节点请求所述用户标识对应的用户信用数据。

35 在一种可能的实现方式中，所述收发模块，具体用于接收至少两个提供节点发送的至少两个数据授权请求，所述至少两个数据授权请求分别与所述至少两个提供节点一一对应，任一数据授权请求用于请求允许所述使用节点使用发送数据授权请求的提供节点提供的所述用户标识对应的用户信用数据；

其中，所述使用节点用于分别向所述至少两个提供节点请求所述用户标识对应的用户

信用数据,所述用户标识对应的用户信用数据包括:由所述至少两个提供节点分别提供的所述用户标识对应的用户信用数据;

所述提示信息用于请求确认是否允许所述使用节点使用所述至少两个提供节点分别提供的所述用户标识对应的用户信用数据。

5 在一种可能的实现方式中,所述装置还包括:

输入模块,所述输入模块用于通过输入设备接收输入信息,所述输入信息用于确认是否允许所述使用节点使用所述至少两个提供节点所提供的所述用户标识对应的用户信用数据;

10 所述收发模块,还用于在所述输入信息表示允许所述使用节点使用所述至少两个提供节点所提供的所述用户标识对应的用户信用数据时,分别向所述提供节点发送数据授权响应,任一所述数据授权响应用于确认允许所述使用节点使用接收数据授权响应的提供节点所提供的用户标识对应的用户信用数据。

第七方面,本申请还提供一种基于区块链网络的数据确权装置,位于区块链节点,一个或多个处理器;

15 存储器,用于存储一个或多个程序;

当所述一个或多个程序被所述一个或多个处理器执行,使得所述设备实现如上述第一方面中任一项所述的方法。

第八方面,本申请还提供一种基于区块链网络的数据确权装置,位于用户终端或者用户客户端,

20 一个或多个处理器;

存储器,用于存储一个或多个程序;

当所述一个或多个程序被所述一个或多个处理器执行,使得所述设备实现如上述第一方面中任一项所述的方法。

25 第九方面,本申请提供一种计算机可读存储介质,包括计算机程序,所述计算机程序在计算机上被执行时,使得所述计算机执行上述第一方面至第三方面中任一项所述的方法。

第十方面,本申请提供一种计算机程序,当所述计算机程序被计算机执行时,实现上述第一方面至第三方面中任一项所述的方法。

30 附图说明

为了更清楚地说明本申请或现有技术中的技术方案,下面将对实施例或现有技术描述中所需要使用的附图作一简单地介绍,显而易见地,下面描述中的附图是本申请的一些实施例,对于本领域普通技术人员来讲,在不付出创造性劳动性的前提下,还可以根据这些附图获得其他的附图。

35 图1为本申请实施例涉及的一种区块链网络的网络架构的示意图;

图2A为本申请实施例提供的基于区块链网络的数据确权方法应用的系统架构的示意图一;

图2B为本申请实施例提供的基于区块链网络的数据确权方法应用的系统架构的示意图二;

图 3 为本申请实施例提供的基于区块链网络的数据确权方法的交互流程图一；

图 4 为本申请实施例提供的基于区块链网络的数据确权方法的交互流程图二；

图 5 为本申请实施例提供的基于区块链网络的数据确权方法的一种应用架构的示意图；

5 图 6 为本申请实施例提供的基于区块链网络的数据确权方法的交互流程图三；

图 7 为本申请实施例提供的基于区块链网络的数据确权装置的结构示意图一；

图 8 为本申请实施例提供的基于区块链网络的数据确权装置的结构示意图二；

图 9 为本申请实施例提供的区块链节点的结构示意图；

图 10 为本申请实施例提供的用户终端的结构示意图。

10

具体实施方式

为使本申请的目的、技术方案和优点更加清楚，下面将结合本申请中的附图，对本申请中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本申请保护的范围。

15

为了提高用户数据的安全性，本申请提供一种可追溯的数据使用的技术方案。本申请提供的技术方案将基于区块链网络实现。下面首先对区块链网络的系统架构进行示例性说明。

图 1 为本申请实施例涉及的一种区块链网络的网络架构的示意图。

20

如图 1 所示，该网络可以包括多个区块链节点。在本申请实施例中，区块链网络中的各个区块链节点可以同时具有一种或多种网络功能和业务功能。

在区块链网络中，区块链节点按照网络功能可初步划分为：普通节点（peer）、排序节点（Orderer）等。普通节点通常可被部署实现一定的业务功能。在一些场景中，一个区块链节点可以既是普通节点，也是排序节点。

25

按照网络功能的具体不同，可以将区块链网络中的普通节点划分为以下几种类型：验证/提交节点（Committer peer）、背书节点（Endorse peer）、领导节点（Leader peer）、锚点节点（Anchor peer）。其中，验证/提交节点可用于提交交易，以及，接收交易信息（也可称为交易块），并在交易信息被写入本地存储的账本前对交易信息进行验证；背书节点可用于根据本节点上安装的智能合约（chain code），生成针对数据交易的数字签名；领导节点可用于当本组织（在一通道中）包括多个区块链节点时，将来自排序节点的交易信息（交易事务）分配给组织中的验证/提交节点；锚点节点可用于实现组织内的节点与组织外的节点的通信。

30

区块链网络的一个重要概念是账本（ledger），也可以称为共享账本。账本用于记录区块链网络中的节点发送或者接收的信息。账本可以通过区块链（block chain）记录通信消息。区块链由若干区块组成，每个区块可以包含一段时间的交易信息，区块链网络中的区块是按照生成的顺序依次连接的。区块链网络中需要保障有至少两个区块链节点上存储账本或者账本副本，本地存储有账本或者账本副本的区块链节点可以称为记账节点，区块链网络中的所有区块链节点都可以是记账节点。区块链中的区块的顺序是不允许改变的，如果任一记账节点存储的区块链中的区块的顺序或者内容

35

发生改变，该记账节点与其他记账节点上存储的区块链就会不一致，这一机制可以保证区块链网络中记录的信息的完整、正确性、不可修改性。

排序节点可以用于进行共识处理，示例性地，排序节点可以对区块链网络中的通信信息进行校验，在校验通过时生成区块，排序节点还可以用于确认区块链网络中生成区块的顺序，并将网络中生成的区块发送至各个记账节点，以使记账节点按照区块的生成顺序将区块加入区块链。

利用区块链网络中与账本有关的技术，可以实现将通过区块链网络中传输的通信消息以区块的形式存储在账本（即存储在区块链中），进而实现对应用场景中涉及的通信消息的可追溯需求。本申请实施例将在下面的部分进行详细说明。

需要说明的是，一个区块链节点可以同时具有上述一种或多种类型的普通节点的网络功能。示例性地，一个区块链节点可以同时是提交节点、背书节点、锚点节点、记账节点。

在区块链网络中，普通节点可被部署用于实现一个或多个网络设备的业务功能。

在实现网络设备的业务功能时，区块链网络中的普通节点可以被划分为一个或多个组织，每个组织可以包括一个或多个普通节点，一个组织中的普通节点可以单独或者相互配合以实现某一网络设备的业务功能，组织中的普通节点还可单独或者相互配合以实现该组织在区块链网络中的一些网络功能。示例性的，各个组织中的节点可以通过广域网（wan）通信。

在本申请提供的技术方案中，还将涉及区块链网络的一种相关技术，该技术可称为 fabric 技术，该技术的关键点之一是支持多账本特性。该技术通过在区块链网络中划分通道（channel），来满足系统对账本的保密及隔离方面的需求。channel 可以用于限定区块链节点间数据交互的范围，一个区块链节点仅允许与所属 channel 相同的其他区块链节点通信。在该技术中，每个 channel 可以对应一个账本，该 channel 对应的账本可以被本 channel 中的所有成员访问。当区块链网络中划分若干 channel 时，区块链网络中的区块链节点可以具有所属 channel 这一属性，需要说明的是，一个区块链节点可以对应一个或多个 channel，即一个区块链节点可以属于一个或多个 channel，当一个区块链节点的所属 channel 属性表明该区块链节点对应某一 channel 时，该区块链节点可以称为该 channel 的一个成员，当一个区块链节点的所属 channel 属性表明该区块链节点对应多个 channel 时，该区块链节点可以分别是多个 channel 的成员。

举例来说，区块链网络可以包括多个区块链节点，其中，多个区块链节点中属于 channel1 的区块链节点可以为 A1 个，A1 大于或者等于 2；多个区块链节点中属于 channel2 的区块链节点可以为 A2 个，A2 大于或者等于 2；对于 channel1 来说，A1 个区块链节点中的 B1 个区块链节点可以存储有 channel1 的账本；B1 大于或者等于 2，且 B1 小于或者等于 A1。则 channel1 中的 A1 个区块链节点可以被允许访问 channel1 的账本，channel2 中的 A2 个区块链节点可以被允许访问 channel2 中账本。

需要说明的是，一个区块链节点所属的 channel 可以有一个或多个，不同 channel 中的区块链节点可以全部不同或者部分不同。在本申请其他实施例中还将结合本申请的实际应用场景对支持 channel 的区块链网络进行示例性说明，此处不再赘述。

下面结合本申请实施例的实际应用场景进行示例性说明。

图 2A 为本申请实施例提供的基于区块链网络的数据确权方法应用的系统架构的示意图一。如图 2A 所示，该系统可以称为数据确权系统，该系统可以包括：区块链网络 100 和用户终端 10。其中，区块链网络 100 可以包括多个区块链节点 20，用户终端的数量可以为一个或多个。区块链网络中的区块链节点可以用于实现多个有业务功能的网络设备。用户终端上可以部署一个或多个用户客户端，部署在用户终端上的用户客户端可以与区块链网络中通过区块链节点实现的各个网络设备进行业务交互。

在本申请实施例的实际应用场景中，使用用户终端或者用户客户端的用户可以对一个用户标识。举例来说，一个用户可以使用一个或多个用户终端，也就是说，一个用户终端可以对应一个用户标识，或者，多个用户终端可以对应的同一个用户标识。每个用户终端上可以部署一个或多个用户客户端，用户客户端对应的用户标识可以为该用户客户端上登录的用户账户对应的用户标识，也就是说，一个用户客户端可以对应一个用户标识，或者，多个用户客户端可以对应同一个用户标识。在一示例中，一个用户所使用的各个用户终端，与部署在该用户所使用的各个用户终端上的用户客户端，可以对应同一用户标识。

在本申请实施例的一种应用场景中，示例性的，系统可以包括用户终端 T1、T2、T3、T4，其中，各个用户终端上部署的用户客户端可以包括 C1、C2、C3、C4、C5、C6、C7。表 1-1 为用户、用户终端、用户客户端以及通过用户客户端通信的网络设备之间的对应关系的一种示意。

表 1-1

用户	用户终端	用户客户端	通过用户客户端通信的网络设备
用户 1	T1	C1	网络设备 1
用户 1	T1	C2	网络设备 2
用户 1	T1	C3	网络设备 3
用户 2	T2	C4	网络设备 1
用户 2	T2	C5	网络设备 2、网络设备 3
用户 2	T3	C6	网络设备 4
用户 3	T4	C7	网络设备 1、网络设备 2、网络设备 3、网络设备 4

如表 1-1 所示，用户 1 可以使用用户终端 T1，T1 上安装有 C1、C2、C3 三个用户客户端，用户客户端 C1、C2、C3 分别用于与网络设备 1、网络设备 2、网络设备 3 进行通信。用户 2 可以使用用户终端 T2 和 T3，T2 上安装的用户客户端 C4 可用于与网络设备 1 进行通信，T2 上安装的用户客户端 C5 可以用于与网络设备 2 和网络设备 3 进行通信，T3 上安装的用户客户端 C6 可以与网络设备 4 进行通信，用户 3 可以使用用户终端 T4，T4 上安装的用户客户端 C7 可以用于与网络设备 1、网络设备 2、网络设备 3、网络设备 4 进行通信。

图 2B 为本申请实施例提供的基于区块链网络的数据确权方法应用的系统架构的示意图二。如图 2B 所示，区块链网络中的各个区块链节点可以用于实现一定的网络设备的业务功能。各个网络设备对应的区块链节点可以通过对应的区块链客户端进行维护。

示例性的，在本申请实施例的一种应用场景中，区块链网络可以包括：普通节点 P1、P2、P3、P4、P5、P6、P7。P1 和 P2 所属组织对应的网络设备可以分别为数据使用商服务器 U1 和 U2，P3、P4 和 P5 所属组织对应的网络设备分别为数据提供商服务器 V1、V2 和 V3。此外，P6 和 P7 所属组织对应的网络设备可以为数据代理商服务器 W1、W2。

举例来说，上述数据使用商可以为银行等向用户提供业务服务的机构，如工商银行、农业银行、建设银行，数据提供商可以为电信运营商、互联网交易平台等存储有用户的各种信用记录的机构，如中国移动、中国联通、京东商城、淘宝网、支付宝等。用户终端上可以安装任一银行客户端，用户可以在银行客户端进行操作，以向银行发起业务请求。

为了便于说明，对应的网络设备的类型为数据使用商服务器的普通节点 P1 和 P2 可以称为使用节点，对应的网络设备的类型为数据提供商服务器的普通节点 P3、P4 和 P5 可以称为提供节点，对应的网络设备的类型为数据代理商服务器的普通节点 P6 可以称为代理节点。在本申请实施例中，代理节点不是区块链网络中必须存在的节点。

在本申请实施例的实际应用场景中，使用节点可以与部署在用户终端上的用户客户端通信，使用节点可以与一个或多个提供节点通信，提供节点可以与部署在用户终端上的用户客户端通信。举例来说，用户终端上可以安装有与一个或多个使用节点进行通信的用户客户端，用户终端可以基于用户客户端与使用节点上的服务端进行通信，例如，使用节点为银行服务器，则用于与使用节点通信的用户客户端可以为手机银行客户端，此外，用户终端上还可以安装有与一个或多个提供节点进行通信的用户客户端，例如，提供节点为运营商服务器，则用于与提供节点通信的客户端可以为运营商手机营业厅客户端。表 1-2 为部署在用户终端上的用户客户端与具有各种业务功能的区块链节点进行业务交互时的对应关系的一种示意。

表 1-2

用户	用户终端	用户客户端	用户客户端支持通信的区块链节点	区块链节点类型	通过区块链节点实现的网络设备对应的组织名称	用户客户端的类型示意
用户 1	T1	C1	U1	使用节点	工商银行	手机银行客户端
用户 1	T1	C2	V1	提供节点	中国移动	运营商手机营业厅客户端
用户 1	T1	C3	U2	使用节点	建设银行	手机银行客户端
用户 2	T2	C4	U1	使用节点	工商银行	手机银行客户端
用户 2	T2	C5	V1、V2	提供节点	中国移动、中国联通	运营商手机营业厅客户端
用户 2	T3	C6	V3	提供节点	中国电信	运营商手机营业厅客户端
用户 3	T4	C7	U1、V1、V3	使用节点、提供节点	工商银行、中国移动、中国电信	综合业务客户端

如表 1-2 所示，用户客户端 C1 可以用于与使用节点 U1 进行通信，用户客户端 C5 可以与提供节点 V1 和 V2 进行通信，用户客户端 C7 可以与使用节点 U1 及提供节点 V1 和 V3 进行通信。

在本申请实施例的实际应用场景中，区块链网络中的各节点的业务功能可以示例如下。

使用节点，可以用于根据携带用户标识的业务请求（例如，从接收携带用户标识的业务请求），确认需要的用户标识对应的用户信用数据，以及，获取用户标识对应的用户信用数据，并根据获取的用户信用数据对携带用户标识的业务请求进行处理。举例来说，使用节点可以接收携带用户标识的业务请求，之后，向提供节点发送数据交易请求，该数据交易请求可以用于请求携带用户标识的业务请求所需的用户标识对应的用户信用数据，然后，接收由提供节点提供的该用户标识对应的用户信用数据，并根据接收到的数据进行业务处理。在本申请实施例中，用户标识对应的用户信用数据可以是指使发送业务请求的用户客户端上登录的用户标识对应的用户信用数据，或者，使用发送业务请求的用户终端的用户的用户标识对应的用户信用数据，例如，用户的征信报告、电信业务使用记录、生活缴费记录等等。

提供节点，可以用于提供海量的用户信用数据。举例来说，提供节点可以接收来自任一使用节点的数据交易请求，之后，根据数据交易请求中的用户标识，向用户标识对应的用户客户端发送数据授权请求，该数据授权请求可用于请求确认是否允许使用节点使用提供节点提供的该用户标识对应的用户信用数据，然后，在接收到用户客户端发送的数据授权响应时，若该数据授权响应表明确认数据授权，即确权成功时，提供节点向使用节点发送使用节点之前请求的用户标识对应的用户信用数据。

在本申请实施例的一种实际应用场景中，系统中还可以部署有代理节点。系统中的使用节点可以与一个或多个代理节点通信，代理节点可以与一个或多个提供节点通信。

代理节点，可以预先与提供节点签订数据代理合约，数据代理合约可以约定该代理节点从提供节点获取并允许向使用节点交易的用户信用数据的范围、期限等信息。在系统中部署有代理节点时，使用节点可以向代理节点发送数据交易请求，代理节点可以在确认使用节点请求交易的数据属于该代理节点的代理范围时，向提供节点发送数据交易请求，相应地，提供节点在从用户客户端获取数据授权时，可以将使用节点请求的用户信用数据发送给代理节点，由代理节点发送给使用节点。

在区块链网络的多个区块链节点中，上述部署有一定业务功能的区块链节点可以称为第一区块链节点。在区块链网络中的多个区块链节点中还可以包括一种区块链节点，该区块链节点可以被称为共识节点。

该共识节点，可以用于接收区块链网络中传输的通信信息，并将通信信息记录在区块链网络的账本中。

需要说明的是，在区块链网络中，区块链节点之间的通信信息是采用广播的方式传播的，也就是说，一个区块链节点向另一个区块链节点发送任一通信信息时，会向相邻的其他区块链节点也发送该通信信息。也就是说，共识节点可以是除了发送某一通信信息或者接收某一通信信息的一个区块链节点。举例来说，共识节点，可以用于

在接收到区块链网络中传输的任一通信信息时，对通信信息中携带的发送方信息进行校验，在确认该通信信息确实是由该发送方发送的时，确认通信信息校验通过，之后，共识节点对校验通过的通信信息进行打包，得到区块，并将包含通信信息的区块发送给区块链网络中的记账节点，以使记账节点将通信信息以区块的形式记录在记账节点本地存储的账本中。在本申请实施例中，共识节点可以是除了使用节点、提供节点、代理节点之外的区块链节点。示例性地，共识节点可以是区块链网络中具有排序节点的网络功能的区块链节点。

下面对本申请实施例的实际应用场景中的多个区块链节点所属 channel 的划分进行示例性说明。在本申请实施例的实际应用场景中，当使用节点、或者、提供节点为多个时，还可以在区块链网络中划分多个 channel。

表 2-1 为多个区块链节点所属 channel 的一种示意。

表 2-1

channel 编号	使用节点	代理节点	提供节点
channel1	U1	-	V1
channel1	U1	-	V2
channel1	U1	-	V3
channel2	U2	-	V1
channel2	U2	-	V2
channel2	U2	-	V3

其中，channel1、channel2 中的区块链节点部分相同。如表 2-1 所示，channel1 的成员可以包括使用节点 U1、提供节点 V1、V2 和 V3，则 U1 与 V1 之间信息、U1 与 V2 之间的信息、U1 与 V3 之间的信息可以记录在 channel1 对应的账本中。channel2 的成员可以包括使用节点 U2、提供节点 V1、V2 和 V3，则 U2 与 V1 之间信息、U2 与 V2 之间的信息、U2 与 V3 之间的信息可以记录在 channel2 对应的账本中。需要说明的是，U2 不能访问 channel1 的账本，U1 不能访问 channel 的账本。

表 2-2 为多个区块链节点所属 channel 的另一种示意。

表 2-2

channel 编号	使用节点	代理节点	提供节点
channel1	U1	W1	V1
channel1	U1	W1	V2
channel1	U1	W1	V3
channel2	U2	W2	V1
channel2	U2	W2	V2
channel2	U2	W2	V3

其中，与表 1 不同之处在于，系统中还部署有代理节点 W1、W2，如表 2-2 所示，channel1 的成员可以包括使用节点 U1、代理节点 W1、提供节点 V1、V2 和 V3，则 U1 与 W1 之间的信息、W1 与 V1 之间的信息、W1 与 V2 之间的信息、W1 与 V3 之间的信息可以记录在 channel1 对应的账本中。channel2 的成员可以包括使用节点 U2、代理节点 W2、提供节点 V1、V2 和 V3，则 U2 与 W2 之间的信息、W2 与 V1 之间信

息、W2 与 V2 之间的信息、W2 与 V3 之间的信息可以记录在 channel2 对应的账本中。需要说明的是，U2、W2 不能访问 channel1 的账本，U1、W1 不能访问 channel2 的账本。

5 下面对本申请实施例提供的基于区块链网络的数据确权方法进行示例性说明。

图 3 为本申请实施例提供的基于区块链网络的数据确权方法的交互流程图一。本申请实施例涉及用户终端、使用节点、提供节点和共识节点。如图 3 所示，本申请实施例的步骤可以包括：

S301，用户终端上的用户客户端向使用节点发送携带用户标识的业务请求。

10 其中，示例性地，用户终端上可以安装有可用于与使用节点通信的第一用户客户端，用户终端可以利用该第一用户客户端向使用节点发送业务请求，使用节点上可以运行有服务端。业务请求中携带的用户标识可以是用户客户端或者用户终端对应的用户标识。

S301-A，使用节点向共识节点发送业务请求。

15 其中，使用节点可以向共识节点发送业务请求以及发送业务请求的发送方的信息，即用户客户端或者用户终端的标识。

使用节点位于区块链网络中，当使用节点接收到用户客户端发送的业务请求后，使用节点可以以广播的方式通过与自身相连的通信链路向区块链网络中的共识节点发送业务请求，以使共识节点将业务请求进行校验，在校验通过时对业务请求进行打包，生成区块，并将区块发送给区块链网络中的记账节点，以使记账节点可以将业务请求以区块的形式记录在区块链网络的账本中。对于步骤 S301-A 来说，共识节点可以是区块链网络中除了使用节点之外的其他任一区块链节点。

需要说明的是，在本申请实施例中，区块链网络中的各个区块链节点之间可以利用区块链网络中的通信链路传输节点之间的通信信息。区块链网络中的各个区块链节点均可以通过广播的方式传播通信信息。区块链网络中的共识节点可以有一个或多个，任一共识节点可以对从另一区块链节点接收到的通信信息进行校验，在校验通过时，将在区块链网络中接收到的通信信息记录在区块链网络的账本中。

S301-C，共识节点对业务请求进行校验，在校验正确时，将业务请求记录在账本中。

30 其中，若共识节点是从使用节点接收到业务请求，则共识节点在确认业务请求中携带的发送方信息为使用节点时，确认校验成功。

需要说明的是，在本申请实施例中，共识节点自身可以不是记账节点，则共识节点可以将接收到的通信信息打包为区块，发送给记账节点，以使记账节点将通信信息以区块的形式记录在记账节点本地存储的账本中。

35 S302，使用节点根据业务请求，确定需要获取的用户标识对应的用户信用数据。

其中，示例性地，使用节点可以根据业务请求的业务标识确定需要的用户信用数据的标识。

S303，使用节点向提供节点发送数据交易请求。

其中，示例性地，数据交易请求可以包括：用户标识、用户信用数据的标识、用

户终端申请的业务的业务标识等。

S303-A, 使用节点向共识节点发送数据交易请求。

其中, 使用节点可以采用与步骤 S301-A 中发送业务请求相似的方式发送数据交易请求。

5 S303-B, 提供节点向共识节点发送数据交易请求。

其中, 提供节点可以采用与步骤 S303-A 中使用节点发送数据交易请求相似的方式来发送数据交易请求。

需要说明的是, 本申请实施例中的 S303-A 和 S303-B 可以任选其一执行。步骤 S303-B 与步骤 S303-A 中的共识节点可以是区块链网络中的同一共识节点, 也可以是不同的共识节点。对于步骤 S303-B 来说, 该步骤中的共识节点可以是区块链网络中除了提供节点之外的任一区块链节点。

S303-C, 共识节点对数据交易请求进行校验, 在校验正确时, 将数据交易请求记录在账本中。

其中, 步骤 S303-C 与步骤 S301-C 类似, 无论共识节点是从使用节点还是提供节点接收到数据交易请求, 共识节点对数据交易请求中携带的发送方的信息进行校验, 在确认数据交易请求的发送方是使用节点时, 确认校验成功。共识节点将校验成功的数据交易请求记录在账本中的方式与步骤 S301-C 中将业务请求记录在账本中的方式相似。

需要说明的是, 若使用节点与提供节点之间的通信链路经过该共识节点, 则在步骤 S303 中使用节点可以通过共识节点向提供节点发送数据交易请求, 则共识节点在接收到数据交易请求之后, 一方面可以将数据交易请求转发给提供节点, 另一方面可以对数据交易请求进行校验和在账本中记录的处理过程。

S304, 提供节点向用户终端上的用户客户端发送数据授权请求。

其中, 示例性地, 用户终端上可以部署有用于与提供节点进行通信的第二用户客户端。第二用户客户端上登录的用户账户对应的用户标识与第一用户客户端上登录的用户账户对应的用户标识相同。第二用户客户端和第一用户客户端也可以是同一用户客户端, 该用户客户端既支持与使用节点进行也能够支持与提供节点进行通信。数据授权请求可以用于请求确认是否允许使用节点使用提供节点所提供的用户标识对应的用户信用数据。在一示例中, 数据授权请求可以具体用于请求确认是否允许使用节点在接收到第一用户客户端发送的第一业务的业务请求时, 使用提供节点所提供的用户标识对应的用户信用数据。示例性的, 数据授权请求可以包括: 使用节点的标识、用户标识、用户信用数据的标识、业务请求的业务标识等。

S304-A, 提供节点向共识节点发送数据授权请求。

其中, 提供节点可以采用与 S303-A 中使用节点发送数据交易请求相似的方式发送数据授权请求。

S304-C, 共识节点对数据授权请求进行校验, 在校验正确时, 将数据授权请求记录在账本中。

其中, 步骤 S304-C 与步骤 S303-C 类似, 共识节点对数据交易请求中携带的发送方的信息进行校验, 在确认数据授权请求的发送方是提供节点时, 确认校验成功。共

识节点将校验成功的数据授权请求记录在账本中的方式与步骤 S303-C 中将数据交易请求记录在账本中的方式相似。

S305, 用户终端上的用户客户端通过输出设备输出提示信息, 提示信息用于请求确认是否允许使用节点使用提供节点提供的用户信用数据。

5 其中, 输出设备可以是用户终端上的显示屏、音箱、耳机等。举例来说, 用户终端上可以安装有用于与提供节点通信的第二用户客户端, 并在第二用户客户端的显示界面上可以显示用于请求用户确认是否允许使用节点使用提供节点提供的用户信用数据的提示信息。示例性地, 提示信息可以包括: 使用节点的标识、用户标识、用户信用数据的标识、业务请求的业务标识, 以及, 是否同意授权的选择按钮等。

10 S306, 用户终端上的用户客户端通过输入设备接收输入信息, 输入信息用于确认是否允许使用节点使用提供节点提供的用户信用数据。

其中, 输入设备可以是具有触摸功能的显示屏、键盘、按钮、麦克风等。示例性地, 第二用户客户端可以在显示界面中接收用户在显示屏上的触摸操作, 例如, 若用户点击屏幕上的“同意”按钮, 则输入信息可以为确认允许授权, 若用户点击屏幕上的“拒绝”按钮, 则输入信息可以为不允许授权。

15 S307, 用户终端上的用户客户端向提供节点发送数据授权响应。

其中, 示例性地, 数据授权响应可以携带用户终端上的第二用户客户端确认允许或者确认不允许使用节点使用提供节点所提供的用户信用数据的指示信息。示例性地, 数据授权响应可以包括: 使用节点的标识、用户标识、用户信用数据的标识、业务请求的业务标识, 以及, 是否同意授权的指示信息等。在一些场景中, 第二用户客户端也可以仅在输入信息表示用户允许授权时发送数据授权响应。

20 S307-B, 提供节点向共识节点发送数据授权响应。

其中, 提供节点可以在接收到用户终端上的第二用户客户端发送的数据授权响应后, 向共识节点数据授权响应。

25 S307-C, 共识节点对数据授权响应进行校验, 在校验正确时, 将数据授权响应记录在账本中。

其中, 与步骤 S304-C 类似, 共识节点可以对数据授权响应的发送方进行校验, 在确认发送方为用户终端上的第二用户客户端时, 确认校验成功, 并将数据授权响应记录在账本中。

30 S308, 提供节点获取用户标识对应的用户信用数据。

其中, 在本申请实施例的一种实施方式中, 提供节点可以在确认数据授权响应表示第二用户客户端允许使用节点使用提供节点提供的用户信用数据时, 获取所需的用户信用数据。在另一种实施方式中, 需要说明的是, 步骤 S304 至步骤 S307-C 可以不是本申请实施例必须执行的步骤, 示例性地, 提供节点在接收到使用节点的数据交易请求之后, 根据自身与使用节点预先签订的数据交易协议, 确定使用节点是否具有使用所请求的用户标识对应的用户信用数据的使用权限, 示例性地, 数据交易协议可以以智能合约(chaincode, 也称为链码)的形式存储于提供节点和使用节点上, 数据交易协议中可以约定使用节点允许使用的用户标识的范围、用户信用数据的标识的范围、用户信用数据的使用期限等。

提供节点获取用户信用数据可以有多种方式，例如，提供节点可以从提供节点自身的数据库或者自身连接的提供商数据服务器获取用户标识对应的用户信用数据。在一些场景中，提供商数据服务器可以位于区块链网络中也可以位于区块链网络之外。举例来说，提供商可以是电信运营商，如中国移动、中国联通、中国电信，则中国移动对应的提供节点提供的用户信用数据可以是该用户终端对应的用户使用中国移动的电信服务时的一些信用记录，例如，充值记录、欠费记录、用户星级、是否属于黑名单、是否发送恶意短信或呼出骚扰电话等。

S309，提供节点向使用节点发送携带用户标识对应的用户信用数据的数据交易响应。

其中，提供节点可以向使用节点发送数据交易响应，示例性地，数据交易响应中可以包括：用户标识、用户信用数据的标识、用户信用数据的使用期限、允许使用节点使用用户信用数据的业务标识等。

S309-A，提供节点向共识节点发送数据交易响应。

S309-B，使用节点向共识节点发送数据交易响应。

其中，步骤 S309-A 和步骤 S309-B 与 S303-A 和 S303-B 类似。

S309-C，共识节点对数据交易响应进行校验，在校验正确时，将数据交易响应记录在账本中。

其中，步骤 S309-C 与步骤 S303-C 类似。

S310，使用节点根据用户标识对应的用户信用数据，对携带用户标识的业务请求进行处理。

其中，使用节点根据获取到的用户信用数据对业务请求进行处理，在用户信用数据满足业务对用户信用水平的需求时，向用户终端上的第一用户客户端提供所申请的业务对应的服务。

S311，使用节点向用户终端上的用户客户端发送业务处理结果。

在本申请实施例中，在上述各种通信信息被记录在账本中之后，区块链网络中的区块链节点可以被允许访问账本中的通信信息。

在本申请实施例中，共识节点和记账节点的数量可以为多个，任一共识节点在对接收到的任一通信信息进行校验通过后，可以在区块链网络中向其他区块链节点广播校验结果，任一记账节点在以区块的形式存储上述任一通信信息时，可以以广播的方式通知区块链网络中其他记账节点同步记录该通信信息，以保证区块链网络中各个记账节点中存储的账本的一致性。

在本申请实施例中，提供节点的数量可以为多个，相应地，用户标识对应的用户信用数据可以包括由多个提供节点分别提供的该用户标识对应的用户信用数据，则使用节点可以向多个提供节点分别发送数据交易请求，任一数据交易请求可用于请求获取接收数据交易请求的提供节点提供的该用户标识对应的用户信用数据。示例性地，使用节点可以为工商银行，多个提供节点可以为中国电信、中国移动、中国联通等运营商，则使用节点需要的用户信用数据可以包括该用户标识分别在中国电信、中国移动、中国联通的数据库中记录的用户信用数据，例如，张某在中国电信、中国移动、中国联通的用户信用数据。

需要说明的是，上述实施例中各个区块链节点与共识节点之间的交互步骤以及共识节点的处理步骤不是本申请必须执行的步骤，在实际应用中，可以根据可追溯的需求，如哪些通信信息需要记录在账本中，在使用节点、提供节点上进行设置，在接收或发送需要记录在账本中的通信信息后，向共识节点发送需要记录的通信信息。此外，对于同一条通信信息，可以由发送该通信信息的区块链节点向共识节点发送，也可以由接收该通信信息的区块链节点向共识节点发送。对于区块链节点与用户终端上的用户客户端之间的交互信息，可以设置由区块链节点向共识节点发送。

在本申请提供的技术方案中，用户客户端、使用节点、提供节点之间交互的通信信息均可以记录在区块链网络中的账本中，从而可以实现用户信用数据的使用过程可追溯。因此，本申请提供的技术方案提高了用户信用数据的安全性。

不仅如此，在本申请提供的技术方案中，在提供节点管理用户信用数据并与使用节点签订有数据交易协议的基础上，提供节点向使用节点提供用户信用数据之前，提供节点再次向用户客户端进行数据是否授权的确认，使得用户能够及时的了解自身用户数据使用的情况，从而可以实现用户信用数据的使用过程在用户终端侧的实时可追溯。进而可以进一步提高用户信用数据的安全性。

本申请实施例还提供一种实施方式，该实施方式涉及多个通道，示例性地，区块链网络可以包括： X 个通道；所述区块链网络中的区块链节点可以分别对应 X 个通道中的一个或多个通道；其中，多个区块链节点中的第一区块链节点对应的通道可以包括第 i 通道，多个区块链节点中的第二区块链节点对应的通道包括第 i 通道， X 为大于0的整数， i 为大于0且小于或者等于 X 的整数。其中，第一区块链节点可以为通信信息的发送方，第二区块链节点可以为通信信息的接收方，例如，第一区块链节点可以是使用节点、提供节点、代理节点中任意一种。

任一第一区块链节点向共识节点发送通信信息，可以包括：第一区块链节点通过所述第 i 通道向所述共识节点发送第 i 通道的通道信息，以使所述共识节点将所述第 i 通道的通道信息记录在第 i 通道对应的账本中。相应地，第 i 通道的通道信息可以包括：所述第一区块链节点与所述第二区块链节点之间通过第 i 通道传输的信息，以及，所述第一区块链节点或者所述第二区块链节点基于从所述第 i 通道接收的信息向所述用户客户端发送的信息，以及，所述第一区块链节点基于从所述用户客户端接收的信息通过第 i 通道向第二区块链节点发送的信息，以及，所述第二区块链节点基于从所述用户客户端接收的信息通过第 i 通道向所述第一区块链节点发送的信息中至少一种。

在一种实际应用中，区块链网络可以包括 M 个使用节点， M 个使用节点分别对应 X 个通道中的一个通道，任一使用节点通过自身对应的通道与提供节点传输信息；所述共识节点对应一个或多个通道。所述第一区块链节点为 M 个使用节点中对应的通道为第 i 通道的第 j 个使用节点，所述第二区块链节点为通过第 i 通道与第 j 个使用节点传输信息的提供节点；或者，所述第一区块链节点为与对应的通道为第 i 通道的第 j 个使用节点通过第 i 通道传输信息的提供节点，所述第二区块链节点为第 j 个使用节点；其中， M 为大于0的整数， j 为大于0且小于或者等于 M 的整数。

下面对利用多个通道实现通信信息存储的相互隔离进行示例性地说明。

图 4 为本申请实施例提供的基于区块链网络的数据确权方法的交互流程图二。本申请实施例可以涉及用户终端 T1，多个使用节点 U1、U2，提供节点 V1，以及，共识节点 Z1、Z2，其中，用户终端 T1 上可以部署用于与各个使用节点和提供节点进行通信的用户客户端。

需要说明的是，在本申请实施例中，U1 和 U2 对应的通道分别为 channel1 和 channel2，T1 与 U1、U1 与 V1、U1 与 Z1 之间以及 V1 与 Z1 之间与 U1 有关的通信信息使用 channel1 的通信链路传输，T1 与 U2、U2 与 V1、U2 与 Z2 之间以及 V1 与 Z2 之间与 U2 有关的通信信息使用 channel2 的通信链路传输，共识节点 Z1 和 Z2 本地分别存储有 channel1 和 channel2 的账本。由于一个 channel 的账本仅允许本 channel 的成员访问，以此可以保证各个 channel 保持的通信信息的相互隔离。

如图 4 所示，本申请实施例的步骤可以包括：

S401，用户终端 T1 向使用节点 U1 发送携带用户标识的第一业务请求。

其中，示例性地，用户终端 T1 可以通过用户客户端 C1 向 U1 发送第一业务请求，用户客户端 C1 支持与 U1 之间的通信。第一业务请求携带用户标识为用户 1，业务标识为业务 1。

S402，用户终端 T1 向使用节点 U2 发送携带用户标识的第二业务请求。

其中，示例性地，用户终端 T1 可以通过用户客户端 C3 向 U2 发送第一业务请求，用户客户端 C3 支持与 U2 之间的通信。第二业务请求携带用户标识为用户 1，业务标识为业务 2。

S401-B，使用节点 U1 向共识节点 Z1 发送第一业务请求。

S401-C，共识节点 Z1 将第一业务请求写入 channel1 对应的账本中。

S402-B，使用节点 U2 向共识节点 Z2 发送第二业务请求。

S402-C，共识节点 Z2 将第二业务请求写入 channel2 对应的账本中。

S403，使用节点 U1 根据第一业务请求确定需要的用户信用数据的标识为 D1。

其中，示例性的，第一业务请求所需的用户信用数据可以为用户 1 对应的标识为 D1 的用户信用数据。

S404，使用节点 U2 根据第二业务请求确定需要的用户信用数据的标识为 D2。

其中，示例性的，第二业务请求所需的用户信用数据可以为用户 1 对应的标识为 D2 的用户信用数据。

S405，使用节点 U1 向提供节点 V1 发送第一数据交易请求。

其中，第一数据交易请求可以用于请求用户 1 对应的标识为 D1 的用户信用数据。

S406，使用节点 U2 向提供节点 V1 发送第二数据交易请求。

其中，第二数据交易请求可以用于请求用户 1 对应的标识为 D2 的用户信用数据。

S405-A，使用节点 U1 向共识节点 Z1 发送第一数据交易请求。

S405-C，共识节点 Z1 将第一数据交易请求写入 channel1 对应的账本中。

S406-A，使用节点 U2 向共识节点 Z2 发送第二数据交易请求。

S406-C，共识节点 Z2 将第二数据交易请求写入 channel2 对应的账本中。

S407，提供节点 V1 向用户终端 T1 发送第一数据授权请求。

其中，第一数据授权请求携带用户标识为用户 1，业务标识为业务 1，需要的用户信用数据的标识为 D1。在一示例中，提供节点 V1 可以向用户终端 T1 上的用户客户端 C1 发送第一数据授权请求，用户客户端 C1 支持与 U1 和 V1 之间的通信，在另一示例中，提供节点 V1 可以向用户终端 T1 上的用户客户端 C2 发送第一数据授权请求，用户客户端 C2 支持与 V1 之间的通信。

S408，提供节点 V1 向用户终端 T1 发送第二数据授权请求。

其中，第二数据授权请求携带用户标识为用户 1，业务标识为业务 2，需要的用户信用数据的标识为 D2。在一示例中，提供节点 V1 可以向用户终端 T1 上的用户客户端 C3 发送第二数据授权请求，用户客户端 C3 支持与 U2 和 V1 之间的通信，在另一示例中，提供节点 V1 可以向用户终端 T1 上的用户客户端 C4 发送第二数据授权请求，用户客户端 C4 支持与 V1 之间的通信。

S407-A，提供节点 V1 向共识节点 Z1 发送第一数据授权请求。

S407-C，共识节点 Z1 将第一数据授权请求写入 channel1 对应的账本中。

S408-A，提供节点 V1 向共识节点 Z1 发送第一数据授权请求。

S408-C，共识节点 Z2 将第二数据授权请求写入 channel2 对应的账本中。

S409，用户终端 T1 在用户客户端上显示第一数据授权请求并接收第一输入信息。

其中，示例性地，用户终端 T1 可以在用户客户端 C3 上显示第一数据授权请求并接收第一输入信息。

S410，用户终端 T1 在用户客户端上显示第二数据授权请求并接收第二输入信息。

其中，示例性地，用户终端 T1 可以在用户客户端 C4 上显示第二数据授权请求并接收第二输入信息。

S411，用户终端 T1 根据第一输入信息向提供节点 V1 发送第一数据授权响应。

其中，示例性地，用户终端 T1 可以通过用户客户端 C3 向提供节点 V1 发送第一数据授权响应。

S412，用户终端 T1 根据第二输入信息向提供节点 V1 发送第二数据授权响应。

其中，示例性地，用户终端 T1 可以通过用户客户端 C4 向提供节点 V1 发送第一数据授权响应。

S411-B，提供节点 V1 向共识节点 Z1 发送第一数据授权响应。

S411-C，共识节点 Z1 将第一数据授权响应写入 channel1 对应的账本中。

S412-B，提供节点 V1 向共识节点 Z2 发送第二数据授权响应。

S412-C，共识节点 Z2 将第二数据授权响应写入 channel2 对应的账本中。

S413，提供节点 V1 根据第一数据授权响应获取用户信用数据 D1。

其中，提供节点 V1 可以根据第一数据授权响应，获取用户 1 对应的用户信用数据 D1。

S414，提供节点 V1 根据第二数据授权响应获取用户信用数据 D2。

其中，提供节点 V1 可以根据第二数据授权响应，获取用户 1 对应的用户信用数据 D2。

S415，提供节点 V1 向使用节点 U1 发送第一数据交易响应。

其中，第一数据交易响应可以包括用户 1 对应的用户信用数据 D1。在一些场景

中，提供节点 V1 可以将用户标识对应的用户信用数据发送给共识节点，以使共识节点将用户信用数据记录在区块链中，使用节点可以从区块链中获取用户标识对应的用户信用数据。

S416，提供节点 V1 向使用节点 U2 发送第二数据交易响应。

5 其中，第二数据交易响应可以包括用户 1 对应的用户信用数据 D2。

S415-A，提供节点 V1 向共识节点 Z1 发送第一数据交易响应。

S415-C，共识节点 Z1 将第一数据交易响应写入 channel1 对应的账本中。

S416-A，提供节点 V1 向共识节点 Z2 发送第二数据交易响应。

S416-C，共识节点 Z2 将第二数据交易响应写入 channel2 对应的账本中。

10 S417，使用节点 U1 对第一业务请求进行处理。

其中，示例性地，使用节点 U1 根据用户 1 对应的用户信用数据 D1 对第一业务请求进行处理。

S418，使用节点 U2 对第二业务请求进行处理。

15 其中，示例性地，使用节点 U2 根据用户 1 对应的用户信用数据 D2 对第二业务请求进行处理。

S419，使用节点 U1 向用户终端 T1 发送第一业务响应。

其中，示例性地，使用节点 U1 可以向用户终端 T1 上的用户客户端 C1 发送第一业务响应，第一业务响应中可以包括使用节点 U1 对第一业务请求的处理结果。

S420，使用节点 UE2 向用户终端 T1 发送第二业务响应。

20 其中，示例性地，使用节点 U2 可以向用户终端 T1 上的用户客户端 C3 发送第二业务响应，第二业务响应中可以包括使用节点 U2 对第二业务请求的处理结果。

S419-A，使用节点 U1 向共识节点 Z1 发送第一业务响应。

S419-C，共识节点 Z1 将第一业务响应写入 channel1 对应的账本中。

S420-A，使用节点 U2 向共识节点 Z2 发送第二业务响应。

25 S420-C，共识节点 Z2 将第二业务响应写入 channel2 对应的账本中。

在本申请实施例中，各个使用节点、提供节点向共识节点发送通信信息的方式，以及共识节点将接收到的通信信息记录在账本中的方式可以参考前述实施例中的描述，区别仅在于，共识节点将各个 channel 的通信信息写入相应 channel 对应的账本中，此处不再赘述。

30 在本申请实施例提供的技术方案中，使用节点 U1 仅被允许访问 channel1 对应的账本，使用节点 U2 仅被允许访问 channel2 对应的账本，从而可以保证各个使用节点相关的通信的信息仅允许被本 channel 内的成员访问。示例性地，使用节点 U1 可以为工商银行，使用节点 U2 可以为建设银行，则工商银行和建设银行的数据确权过程的通信信息的保存是相互隔离的，工商银行和建设银行不能访问对方银行相关的账本中
35 记录的通信信息。

在本申请实施例中，在一种实施方式中，共识节点 Z1 和 Z2 可以为同一区块链节点，即该共识节点上可以同时保存有 channel1 和 channel2 对应的账本，但是，按照隔离度的需求，使用节点 U1 仍然仅被允许访问共识节点上 channel1 对应的账本中的通信信息，使用节点 U2 仅被允许访问共识节点上 channel2 对应的账本中的通信信息。

在本申请其他实施例中，当系统中部署有代理节点时，代理节点与使用节点和提供节点之间的通信信息也能够按照通信信息对应的通道记录在通道对应的账本中。

本申请实施例的其他技术方案细节和技术效果，可参看图 2 所示实施例中的相关描述，此处不再赘述。

5

下面结合本申请实施例的一些实际应用场景对本申请实施例提供的基于区块链网络的数据确权方法进行示例性说明。

在一种应用场景中，用户 A 可以向数据使用企业申请业务，数据使用企业为了降低业务风险，需对用户做出信用评价，根据用户的信用等级决定是否为用户办理相关业务。数据使用企业可以向数据代理商请求用户 A 的电信数据，数据代理商查看与数据使用企业是否有合作、合作是否到期等确认数据使用企业的权限，若数据使用企业无权限，则向数据使用企业返回拒绝服务，若有权限，则数据代理商向运营商申请用户 A 的数据，运营商查验数据代理商的权限，若运营商检查数据代理商无相应权限，则向数据代理商返回拒绝服务，若数据代理商有权限，则向数据代理商返回用户 A 的数据。之后，数据使用企业可以从数据代理商处获取到用户 A 的数据，并对用户作出信用评价，决定是否办理相关业务。

根据上述业务需要，可以在区块链网络中部署各个组织对应的区块链节点。在实际应用中，数据使用企业（即数据使用商，如银行）可以部署为使用节点，数据提供企业（即数据提供商，如运营商）可以部署为提供节点，数据代理商可以部署为代理节点，用户使用的终端可以为用户终端，用户终端上可以部署用于与各个使用节点、各个提供节点进行通信的一个或多个用户客户端，用户可以通过用户终端上部署的用户客户端向数据使用企业发起携带用户标识的业务请求。

图 5 为本申请实施例提供的基于区块链网络的数据确权方法的一种应用架构的示意图。如图 5 所示，在实际应用的业务场景中，当区块链网络中部署有代理节点时，用户终端上的用户客户端与使用节点之间、使用节点与代理节点之间、代理节点与提供节点、提供节点与用户终端上的用户客户端之间可以分别建立通信连接。使用节点可以通过代理节点与提供节点交互。

在区块链网络中，代理节点的业务功能可以包括以下至少一个：接收使用节点发送的数据交易请求，其中，数据交易请求用于请求用户标识对应的用户信用数据；以及，确认所述使用节点是否具有所述用户标识对应的用户信用数据的访问权限；以及，在确认使用节点具有访问权限时，向提供节点发送数据交易请求；以及，接收提供节点发送的数据交易响应，其中，数据交易响应包括用户标识用户信用数据。

为了实现上述代理节点的业务功能，在一种实施方式中，代理节点可以分别与各个使用节点和各个提供节点签订数据交易合约。代理节点与提供节点之间的数据交易合约可以约定该代理节点允许从某一提供节点获取的用户标识对应的用户信用数据的范围，如用户标识的范围、用户信用数据的标识、使用期限、允许使用用户信用数据的业务标识等。代理节点与使用节点之间的数据交易合约也可以进行类似的约定。任一代理节点可以与多个提供节点分别签订数据交易合约，从而可以向所服务的使用节点提供多个提供节点所分别提供的用户标识对应的用户信用数据。

此外，处于区块链网络中的代理节点与区块链网络中的任一共识节点之间也可以建立有通信连接，代理节点在从使用节点或提供节点接收到通信信息之后，或者，代理节点在向使用节点或提供节点发送通信信息之后，可以将接收或者发送的通信信息发送给共识节点，以使共识节点对从代理节点接收到的通信信息进行校验，并在校验成功时，将从代理节点接收到的通信信息以区块的形式记录在区块链网络的账本中。采用这种部署方式，可以实现区块链网络中代理节点与其他区块链节点之间交互的通信信息可回溯的需求。

示例性地，在部署有代理节点时，本申请实施例提供的数据确权方法的基本流程可以包括下面几个阶段。

其中，区块链网络之间交互通信信息是通过各个区块链节点向区块链网络广播要发送的通信信息实现的，示例性地，作为通信信息的发送方的区块链节点可以向邻近的各个区块链节点发送待发送的通信信息。区块链网络中各个区块链节点按照所部署的业务功能和网络功能相互配合。使用节点、代理节点、提供节点可以通过分别通过数据使用商区块链客户端、数据代理商客户端、数据提供商客户端进行维护。

第一阶段，使用节点向区块链网络发送数据使用请求。

其中，（1）使用节点接收用户终端上的用户客户端发送的业务请求，以及个人数据；（2）使用节点将用户标识（如姓名、身份证号、手机号等）和申请的业务标识打包成消息 M，使用节点使用自身对应的公钥加密，并加上私钥签名，发到其他区块链节点（该其他区块链节点可以是除了使用节点之外的区块链节点）中。

第二阶段，代理节点向区块链网络发送数据使用请求。

其中，（1）代理节点判断使用节点是否具有数据获取权限，若无权限，则结束处理流程，若有，执行（2）；（2）代理节点在消息 M 中添加数据源列表，打包成消息 M1，发送到其他区块链节点（该其他区块链节点可以是除了代理节点之外的区块链节点）。

第三阶段，提供节点向用户终端上的用户客户端申请数据使用权限。

其中，（1）提供节点将数据源列表及数据授权申请发送给用户终端上的用户客户端（例如前述实施例中的第二用户客户端，图中未体现）；（2）用户客户端整合收到的数据授权申请，满足数据源列表的要求如数量和申请方 ID，激活授权操作；（3）用户客户端对每一条数据授权申请签名（表示用户允许提供节点使用数据源列表中的用户数据），并且用对应申请方（即对应的使用节点提供节点）的公钥加密，生成消息 M2，发送到提供节点或者与用户终端相连的其他区块链节点（该其他区块链节点可以是除了提供节点之外区块链节点）。

第四阶段，提供节点将用户数据发送到区块链网络。

其中，（1）提供节点将使用节点的信息（如银行信息）、数据使用范围、经过使用节点的公钥加密的用户数据和私钥签名（即用户终端的签名）打包成消息 M3，发送到其他区块链节点（该其他区块链节点可以是除了提供节点之外的区块链节点）；（2）使用节点收到用户数据（可以对消息 M3 解密，提取其中的用户数据）之后，执行智能合约，执行智能合约的输入为使用节点的信息和用户终端的信息，输出为数据使用交易，使用节点可以将生成的数据使用交易（或者，使用节点可以将提供节点

或者代理节点接收到的用户数据）发到其他区块链节点（该其他区块链节点可以是除了使用节点之外的区块链节点）；（3）使用节点转发用户数据到自身的信用评价系统，对用户标识对应的用户做出信用评价，并根据信用评价结果对用户终端上的用户客户端发送的业务请求进行处理。

5 需要说明的是，各个节点预先已建立合作关系，生成自身对应的公钥和私钥对以及相应整数，同时将各自的公钥在区块链网络中公开。

在本申请实施例中，上述区块链网络中传输的通信消息可以采用统一的消息格式。举例来说，通信信息可以包括以下字段：发送方（sender）、标签（label）、消息（message）等。统一的消息格式可以示例如下：

10 {sender: “”,
label: “”,
message: “”}

下面采用具体的例子对本申请实施例提供的基于区块链网络的数据确权方法的交互过程以及消息格式进行示例性说明。

15 图6为本申请实施例提供的基于区块链网络的数据确权方法的交互流程图三。本申请实施例涉及用户名为张某的用户使用的终端上部署的用户客户端、工商银行区块链节点（即使用节点）、联通运营商区块链节点（即提供节点U1）、移动运营商区块链节点（即提供节点U2）、数据代理商区块链节点（即代理节点W1）和其他区块链节点（即共识节点）。

20 举例来说，本申请实施例的实际业务需求可以包括：张某到工商银行办理贷款业务，工商银行为了降低业务风险，需要使用运营商中存储的张某的用户数据对张某进行信用评价。在具体实施前，工商银行作为数据使用商可以与数据代理商签订合同，建立数据使用关系，数据代理商作为两家运营商提供数据业务的统一对外接口，为数据使用商提供数据服务，两家运营商分别为数据源企业，在经过用户授权的情况下，
25 开放用户数据给数据使用商使用。

如图6所示，本申请实施例的步骤可以包括：

S600，用户客户端向工商银行区块链节点申请业务，提交个人信息。

30 其中，示例性地，用户通过用户客户端可以向工商银行申请贷款业务，提供的个人信息可以包括姓名、身份证号、手机号等。

S601，工商银行区块链节点将张某的个人数据及业务申请打包成消息M，label字段为“bank_request”，加上私钥签名，向其他区块链节点发送消息M。

示例性的，消息M的内容可以为：

35 {sender: “bankID”,
label: “bank_request”,
message: { “name”: “张某”, “ID”: “5555555”, “telephone”: “13243793294”,
“business”: “bank loan” }}

其中，bankID为工商银行的标识，bank_request表示该消息为银行发出的请求，message中的信息可以包括用户标识和所申请的业务标识。

需要说明的是，在本申请实施例中，其他区块链节点可以用于执行前述实施例中共识节点执行的步骤。

S602，其他区块链节点广播消息 M，并验证消息来源，在确认共识之后，将消息 M 写入区块链。

5 其中，示例性地，消息 M 经过其他区块链节点广播后，可以验证消息来源于工商银行，确认共识，将消息 M 写入区块链（即区块链网络的账本）中。

S603，数据代理商区块链节点查验消息 M 中的 label 字段，如果 label 字段的值为“bank_request”，执行 S604，如果 label 字段的值不是“bank_request”，则仅写入交易。

10 S604，数据代理商区块链节点执行智能合约，输入工商银行区块链节点的公钥，判断工商银行区块链节点是否有权限获取用户数据，若有权限，执行 S605。

S605，数据代理商区块链节点生成消息 M1，label 字段为“proxy_request”，message 字段增加数据源列表，向其他区块链节点发送消息 M1。

示例性的，消息 M1 的内容可以为：

15 {sender: “proxyID”，
label: “proxy_request”，
message:{ “name”：“张某”，“ID”：“5555555”，“telephone”：
“13243793294”，“business”：“bank loan”，“data_source_list”:[“移动”，
“联通”]}}

20 其中，proxyID 为数据代理商的标识，proxy_request 表示该消息为数据代理商发出的请求，message 中的信息可以包括用户标识（name、ID、telephone）、所申请的
业务标识（business）和数据源列表（data_source_list）。

需要说明的是，数据代理商区块链节点可以预先与移动运营商区块链节点、联通
运营商区块链节点签订数据代理合同，该数据代理合同可以约定数据代理商节点允许
25 使用的由移动运营商、联通运营商区块链节点管理和提供的用户数据的范围、期限、
应用范围等，其中，应用范围可以包括：允许使用的银行、允许使用的业务标识等。
数据代理商可以在数据代理合同约定的范围，确定本次业务需要获取的数据源列表，
这样可以使得银行方面可以获得尽可能多的用户数据。示例性的，数据代理商代理了
移动运营商和联通运营商的数据，则可以将移动运营商和联通运营商的标识作为数据
30 源列表添加到消息 M1 中。

S606，其他区块链节点广播消息 M1，并验证消息来源，在确认共识之后，将消息 M1 写入区块链。

35 S607-1，联通运营商区块链节点查验消息 M1 中的 label 字段，如果 label 字段的
值为“proxy_request”执行 S607-2，如果 label 字段的值不是“proxy_request”则不执
行操作。

S608-1，移动运营商区块链节点查验消息 M1 中的 label 字段，如果 label 字段的
值为“proxy_request”执行 S608-2，如果 label 字段的值不是“proxy_request”则不执
行操作。

S607-2，联通运营商区块链节点生成消息 M2，label 字段的值为

“user_authorization_request”，message 字段包括数据源列表及数据使用申请，添加联通运营商区块链节点的私钥签名，发送给用户客户端。

示例性的，消息 M2 的内容可以为：

```
{sender: “data_source_ID”,  
label: “user_authorization_request”,  
message:{ “data_source_list”:[ “移动”, “联通” ], “bank” : “bankID” ,  
“msg” : “bankID want to use your personal data” }
```

其中，data_source_ID 为数据源企业的标识（如联通运营商区块链节点、移动运营商区块链节点），user_authorization_request 表示该消息为数据提供商发出的请求（如用户授权请求），message 中的信息可以包括数据源列表（data_source_list）、请求使用用户数据的银行的标识（如工商银行的标识）、请求授权的内容（如工商银行请求使用您的个人信息）。

S608-2，移动运营商区块链节点生成消息 M2'，label 字段的值为

“user_authorization_request”，message 字段包括数据源列表及数据使用申请，添加移动运营商区块链节点的私钥签名，发送给用户客户端。

示例性的，消息 M2'的内容可以为：

```
{sender: “data_source_ID”,  
label: “user_authorization_request”,  
message:{ “data_source_list”:[ “移动”, “联通” ], “bank” : “bankID” ,  
“msg” : “bankID want to use your personal data” }
```

其中，各参数的含义与 S607-2 中的参数含义相同。

S609，用户客户端在收到的数据使用请求的数量及请求方符合数据源列表要求时，激活授权操作。

其中，消息 M2 和消息 M2'可以为数据使用请求，数据使用请求与前述实施例中
使用节点或者代理节点发送给提供节点的数据授权请求的作用相似，均可以请求用户
客户端确认或者知悉自身数据被使用的情况。

示例性的，数据源列表要求可以包含用户客户端已协商同意授权的一个或多个运营商的标识，以及，请求使用的数据的数量的范围。例如，若用户客户端对应的用户为移动运营商用户，则数据源列表要求可以包括移动运营商的标识，请求使用的数量的范围可以包括最近半年内用户欠费次数等。

用户客户端在确认符合数据源列表要求时，可以激活授权操作。在一示例中，激活授权操作可以包括：用户客户端可以在接收到请求使用数据的数据授权请求的运营商的标识以及请求使用的数据的数量符合数据源列表要求时，确认用户确认授权，此时，用户客户端可以在显示界面上向用户显示一条确认授权的提示信息，以提示用户的数据正在被使用。在另一示例中，用户客户端可以在显示界面中显示请求使用数据的运营商的标识和所请求使用的数据的数量、业务等信息，并提示用户确认是否同意授权运营商向银行提供相应用户数据，当用户输入同意授权时，用户客户端确认用户确认授权。

S610，用户客户端在用户确认授权时，对数据使用请求分别签名，并用对应请求

方的公钥加密，生成消息 M3，label 字段的值为“user_authorization”，向各个运营商区块链节点发送消息 M3。

其中，用户客户端对各个运营商区块链节点发送的每个数据使用请求分别进行签名，

- 5 在本申请实施例中，用户客户端可以向各个提供节点发送消息 M3。在一些实施方式中，若用户客户端与区块链网络中的其他区块链节点相连，也可以向其他区块链节点发送消息 M3，当用户客户端直接向其他区块链节点发送消息 M3 时，可以不执行 S611 直接执行 S612。

示例性的，消息 M3 的内容可以为：

10 { sender: username
 label: user_authorization
 message:{ “移动”:M’ ,“联通”:M’ }}

- 15 其中，username 为用户终端对应的用户标识（如张某），user_authorization 表示该消息为用户终端或者用户客户端发出的用户授权（如用户授权响应），message 中的信息可以包括各个数据源（如移动、联通）以及各个数据源对应的经过加密的数据授权请求（如经过用户私钥签名和各个数据源（data_source_ID）的公钥对 M2 消息进行加密得到的 M’ 消息）。

S611，各个运营商区块链节点向其他区块链节点发送消息 M3。

- 20 其中，示例性地，移动运营商区块链节点和联通区块链节点可以分别向其他区块链节点发送消息 M3。

S612，其他区块链节点广播消息 M3，并验证消息来源，在确认共识之后，将消息 M3 写入区块链。

其中，消息 M3 经过其他区块链节点广播后，可以验证消息来源于用户客户端，确认共识，将消息 M 写入区块链（即区块链网络的账本）中。

- 25 S613，各个运营商区块链节点查验消息 M3 中的 label 字段，确认用户签名后，将银行数据、数据使用范围和经过工商银行的公钥加密的用户数据打包，发送给工商银行区块链节点。

其中，

- 30 S614，工商银行区块链节点在收到用户数据后，执行智能合约，输入为工商银行数据和用户数据，生成数据使用交易，发送到其他区块链节点。

S615，工商银行区块链节点将接收到的用户数据转发至信用评价系统，对用户做出信用评价。

- 35 在本申请实施例中，基于上述实施例所示，部署有使用节点、代理节点和提供节点的区块链网络可以与部署于用户终端上的用户客户端进行交互，其中，使用节点可以从用户客户端接收业务请求，然后，区块链网络内部中的使用节点、代理节点以及提供节点各司其职，使用节点确认需要获取的用户终端对应的用户信用数据，代理节点确认请求的数据是否属于代理节点的代理范围，提供节点向用户客户端发送数据授权请求（即数据使用请求），用户客户端通过与用户的人机交互获得用户输入的确认信息，并将授权结果反馈给提供节点。在这个过程中，一方面，区块链网络的账本中

可以记录整个业务流程中各个区块链节点之间的通信信息，同时，区块链网络还可以记录用户客户端与区块链节点之间的通信信息，可见，采用本申请实施例提供的技术方案可以实现用户数据使用过程的完整记录，当使用节点、代理节点、提供节点以及用户客户端之间对用户数据使用过程存在疑问时，可以从区块链网络的账本中获得准备的过程信息。

在本申请实施例中，用户可以使用一个或多个用户终端上部署的一个或多个用户客户端与各个使用节点和提供节点进行通信。在一示例中，用户可以用一个用户客户端与各个提供节点进行通信。

本申请实施例的其他技术方案细节及技术效果可参看前面实施例中的说明，此处不再赘述。

本申请实施例还提供一种基于区块链网络的数据确权装置。

图7为本申请实施例提供的基于区块链网络的数据确权装置的结构示意图一；如图7所示，本申请实施例还提供一种基于区块链网络的数据确权装置700，应用于区块链网络中的第一区块链节点，装置700包括：

收发模块701，用于发送或者接收通信信息；

处理模块702，将所述通信信息记录在区块链网络的账本中；

其中，区块链网络包括多个区块链节点，多个区块链节点包括：使用节点和提供节点；使用节点，用于根据携带有用户标识的业务请求，向提供节点请求用户标识对应的用户信用数据；提供节点，用于向使用节点提供用户信用数据；通信信息包括：第一区块链节点与多个区块链节点中的任一其他区块链节点之间的信息，以及，第一区块链节点与用户客户端之间的信息中至少一种；其中，用户客户端用于向使用节点发送携带有用户标识的业务请求，和/或，用户客户端用于确认是否允许提供节点向使用节点提供用户标识对应的用户信用数据；第一区块链节点为多个区块链节点中的区块链节点。

在一种可能的实施方式中，处理模块702，可以指示收发模块701向共识节点发送通信信息，以使共识节点将通信信息记录在区块链网络的账本中；共识节点为多个区块链节点中除了第一区块链节点之外的区块链节点。

在一种可能的实施方式中，收发模块701，可以具体用于：

向第二区块链节点发送通信信息；或者，

接收第二区块链节点发送的通信信息；或者，

向用户客户端发送通信信息；或者，

接收用户客户端发送的通信信息；

其中，第二区块链节点为多个区块链节点中除第一区块链节点之外的任一其他区块链节点。

在一种可能的实施方式中，第一区块链节点可以为使用节点；用户客户端用于向使用节点发送携带有用户标识的业务请求；

收发模块701，可以具体用于发送或者接收通信信息，其中，通信信息具体包括：使用节点与多个区块链节点中的其他区块链节点之间的信息，以及，使用节点与用户

客户端之间的信息中至少一种；共识节点为多个区块链节点中除使用节点之外的任一区块链节点。

在一种可能的实施方式中，第一区块链节点为提供节点；用户客户端用于确认是否允许提供节点向使用节点提供用户标识对应的用户信用数据；

5 收发模块 701，可以具体用于发送或者接收通信信息，其中，通信信息具体包括：提供节点与多个区块链节点中的其他区块链节点之间的信息，以及，提供节点与用户客户端之间的信息中至少一种；共识节点为多个区块链节点中除提供节点之外的任一区块链节点。

10 在一种可能的实施方式中，第一区块链节点为使用节点；用户客户端用于向使用节点发送携带有用户标识的业务请求；收发模块 701，具体用于以下至少一种：

接收用户客户端发送的携带用户标识的业务请求；

向提供节点发送数据交易请求，数据交易请求用于请求获取用户标识对应的用户信用数据，用户信用数据用于使用节点处理携带有用户标识的业务请求；

15 接收提供节点发送的数据交易响应，数据交易响应包括用户标识对应的用户信用数据。

在一种可能的实施方式中，第一区块链节点为提供节点；用户客户端用于确认是否允许提供节点向使用节点提供用户标识对应的用户信用数据；收发模块 701，具体用于以下至少一种：

20 接收使用节点发送的数据交易请求，数据交易请求用于请求获取用户标识对应的用户信用数据，用户信用数据用于使用节点处理携带有用户标识的业务请求；

向用户客户端发送数据授权请求，数据授权请求用于请求用户客户端允许向使用节点提供用户标识对应的用户信用数据；

接收用户客户端发送的数据授权响应，数据授权响应用于确认是否允许向使用节点提供用户标识对应的用户信用数据；

25 向使用节点发送数据交易响应，数据交易响应包括用户标识对应的用户信用数据。

30 在一种可能的实施方式中，多个区块链节点包括：代理节点；代理节点，用于接收使用节点发送的数据交易请求，数据交易请求用于请求用户标识对应的用户信用数据；以及，确认使用节点是否具有用户标识对应的用户信用数据的访问权限；以及，在确认使用节点具有访问权限时，向提供节点发送数据交易请求；以及，接收提供节点发送的数据交易响应，数据交易响应包括用户标识对应的用户信用数据；

第一区块链节点为代理节点；收发模块 701，具体用于发送或者接收通信信息，其中，通信信息具体包括：代理节点与使用节点之间的信息，代理节点与提供节点之间的信息中至少一种。

35 在一种可能的实施方式中，区块链网络包括：X 个通道；区块链网络中的区块链节点分别对应 X 个通道中的一个或多个通道；其中，第一区块链节点对应的通道包括第 i 通道，区块链网络中的第二区块链节点对应的通道包括第 i 通道；

收发模块 701，具体用于将第 i 通道的通道信息记录在第 i 通道对应的账本中；

第 i 通道的通道信息包括：第一区块链节点与第二区块链节点之间通过第 i 通道

传输的信息, 以及, 第一区块链节点或者第二区块链节点基于从第 i 通道接收的信息向用户客户端发送的信息, 以及, 第一区块链节点基于从用户客户端接收的信息通过第 i 通道向第二区块链节点发送的信息, 以及, 第二区块链节点基于从用户客户端接收的信息通过第 i 通道向第一区块链节点发送的信息中至少一种;

5 其中, X 为大于 0 的整数, i 为大于 0 且小于或者等于 X 的整数。

在一种可能的实施方式中, 区块链网络包括 M 个使用节点, M 个使用节点分别对应 X 个通道中的一个通道, 任一使用节点通过自身对应的通道与提供节点传输信息; 共识节点对应一个或多个通道;

10 第一区块链节点为 M 个使用节点中对应的通道为第 i 通道的第 j 个使用节点, 第二区块链节点为通过第 i 通道与第 j 个使用节点传输信息的提供节点; 或者, 第一区块链节点为与对应的通道为第 i 通道的第 j 个使用节点通过第 i 通道传输信息的提供节点, 第二区块链节点为第 j 个使用节点;

其中, M 为大于 0 的整数, j 为大于 0 且小于或者等于 M 的整数。

15 在一种可能的实施方式中, 区块链网络包括 M 个使用节点, M 个使用节点分别对应 X 个通道中的一个通道, 任一使用节点通过自身对应的通道与提供节点传输信息;

20 多个区块链节点包括: 代理节点; 代理节点, 用于接收使用节点发送的数据交易请求, 数据交易请求用于请求用户标识对应的用户信用数据; 以及, 确认使用节点是否具有用户标识对应的用户信用数据的访问权限; 以及, 在确认使用节点具有访问权限时, 向提供节点发送数据交易请求; 以及, 接收提供节点发送的数据交易响应, 数据交易响应包括用户标识对应的用户信用数据;

25 第一区块链节点为 M 个使用节点中对应的通道为第 i 通道的第 j 个使用节点, 第二区块链节点为与第 j 个使用节点通过第 i 通道传输信息的代理节点; 或者, 第一区块链节点为与对应的通道为第 i 通道的第 j 个使用节点通过第 i 通道传输信息的代理节点, 第二区块链节点为第 j 个使用节点; 或者, 第一区块链节点为与对应的通道为第 i 通道的第 j 个使用节点通过第 i 通道传输信息的代理节点, 第二区块链节点为与第一区块链节点通过第 i 通道传输信息的提供节点;

其中, M 为大于 0 的整数, j 为大于 0 且小于或者等于 M 的整数。

30 在一种可能的实施方式中, 提供节点为运营商服务器; 用户信用数据为用户标识对应的运营商信用数据。

在本申请实施例中, 举例来说, 在装置 700 位于使用节点时, 处理模块 702 可以用于根据业务请求确认需要的用户信用数据的标识, 在装置 700 位于提供节点时, 处理模块 702 可以用于确认使用节点是否具有访问用户标识对应的用户信用数据的权限; 在装置 700 位于代理节点时, 处理模块 702 可以用于确认使用节点是否具有访问提供节点提供的用户标识对应的用户信用数据的权限等, 可参看前面实施例中各个区块链节点执行步骤的描述。

本申请实施例提供的基于区块链网络的数据确权装置可以用于实现前述任一实施例中各个区块链节点执行的方法, 其技术方案细节及技术效果可参见前述实施例中的描述。

图 8 为本申请实施例提供的基于区块链网络的数据确权装置的结构示意图二。

如图 8 所示, 本申请实施例还提供一种基于区块链网络的数据确权装置 800, 应用于用户终端或者用户客户端, 装置 800 包括:

收发模块 801, 用于接收提供节点发送的携带有用户客户端对应的用户标识的数据授权请求, 数据授权请求用于请求允许使用节点使用提供节点提供的用户标识对应的用户信用数据;

输出模块 802, 用于通过输出设备输出提示信息, 提示信息用于请求确认是否允许使用节点使用提供节点提供的用户标识对应的用户信用数据;

其中, 使用节点、提供节点为区块链网络中的区块链节点, 使用节点用于向提供节点请求用户标识对应的用户信用数据。

在一种可能的实施方式中, 收发模块 801, 可以具体用于接收至少两个提供节点发送的至少两个数据授权请求, 至少两个数据授权请求分别与至少两个提供节点一一对应, 任一数据授权请求用于请求允许使用节点使用发送数据授权请求的提供节点提供的用户标识对应的用户信用数据;

其中, 使用节点用于分别向至少两个提供节点请求用户标识对应的用户信用数据, 用户标识对应的用户信用数据包括: 由至少两个提供节点分别提供的用户标识对应的用户信用数据;

提示信息用于请求确认是否允许使用节点使用至少两个提供节点分别提供的用户标识对应的用户信用数据。

在一种可能的实施方式中, 装置 800 还可以包括:

输入模块 802, 输入模块用于通过输入设备接收输入信息, 输入信息用于确认是否允许使用节点使用至少两个提供节点所提供的用户标识对应的用户信用数据;

收发模块 801, 还用于在输入信息表示允许使用节点使用至少两个提供节点所提供的用户标识对应的用户信用数据时, 分别向提供节点发送数据授权响应, 任一数据授权响应用于确认允许使用节点使用接收数据授权响应的提供节点所提供的用户标识对应的用户信用数据。

在本申请实施例中, 装置 800 还可以包括处理模块 804, 举例来说, 处理模块 804 可以用于根据用户的输入信息生成数据授权响应, 可参看前面实施例中用户终端或用户客户端执行步骤的描述。

本申请实施例提供的基于区块链网络的数据确权装置可以用于实现前述任一实施例中各个用户客户端、第二用户客户端执行的方法, 其技术方案细节及技术效果可参见前述实施例中的描述。

本申请实施例还提供一种区块链节点, 所述区块链节点于执行前述实施例中任一所述的数据识别方法中的步骤。在一示例中, 区块链节点可以为服务器或者终端。

本申请实施例还提供一种用户客户端, 所述用户客户端用于执行前述实施例中任一所述的数据识别方法中的步骤。

本申请实施例还提供一种区块链节点, 图 9 为本申请实施例提供的区块链节点的结构示意图。如图 9 所示, 本申请实施例还提供一种区块链节点 900, 包括: 一个或多个处理器 901; 存储器 902, 用于存储一个或多个程序; 当所述一个或多个程序被

所述一个或多个处理器执行，使得所述一个或多个处理器实现如上述前述实施例所述方法中第一区块链节点执行的步骤。示例性地，该区块链节点可以为服务器、终端。在本申请实施例中，区块链节点 900 还可以包括接口 903，用于与设置有用户客户端的用户终端进行通信，此外，服务器和还可以包括总线 904，用于实现服务器内部的通信。

本申请实施例还提供一种用户终端，图 10 为本申请实施例提供的用户终端的结构示意图。如图 10 所示，用户终端 1000，包括：一个或多个处理器 1001；存储器 1002，用于存储一个或多个程序；当所述一个或多个程序被所述一个或多个处理器执行，使得所述一个或多个处理器实现如上述前述实施例所述方法中用户终端及用户终端上部署的用户客户端执行的步骤。在本申请实施例中，用户终端 1000 还可以包括接口 1003，用于与区块链节点进行通信，此外，用户客户端 1000 和还可以包括总线 1004，用于实现内部的通信。

本申请提供一种计算机可读存储介质，包括计算机程序，所述计算机程序在计算机上被执行时，使得所述计算机执行上述实施例中任一项所述的方法。

本申请提供一种计算机程序，当所述计算机程序被计算机执行时，用于执行上述实施例中任一项所述的方法。

在上述实施例中，可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。当使用软件实现时，可以全部或部分地以计算机程序产品的形式实现。所述计算机程序产品包括一个或多个计算机指令。在计算机上加载和执行所述计算机程序指令时，全部或部分地产生按照本申请所述的流程或功能。所述计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。所述计算机指令可以存储在计算机可读存储介质中，或者从一个计算机可读存储介质向另一个计算机可读存储介质传输，例如，所述计算机指令可以从一个网站站点、计算机、服务器或数据中心通过有线（例如同轴电缆、光纤、数字用户线）或无线（例如红外、无线、微波等）方式向另一个网站站点、计算机、服务器或数据中心进行传输。所述计算机可读存储介质可以是计算机能够存取的任何可用介质或者是包含一个或多个可用介质集成的服务器、数据中心等数据存储设备。所述可用介质可以是磁性介质，（例如，软盘、硬盘、磁带）、光介质（例如，DVD）、或者半导体介质（例如固态硬盘 Solid State Disk）等。

权利要求书

1、一种基于区块链网络的数据确权方法，其特征在于，所述方法包括：

区块链网络中的第一区块链节点发送或者接收通信信息；

所述第一区块链节点将所述通信信息记录在区块链网络的账本中；

5 其中，所述区块链网络包括多个区块链节点，所述多个区块链节点包括：使用节点和提供节点；所述使用节点，用于根据携带有用户标识的业务请求，向所述提供节点请求所述用户标识对应的用户信用数据；所述提供节点，用于向所述使用节点提供用户信用数据；所述通信信息包括：所述第一区块链节点与所述多个区块链节点中的任一其他区块链节点之间的信息，以及，第一区块链节点与用户客户端之间的信息中
10 至少一种；其中，所述用户客户端用于向所述使用节点发送携带有所述用户标识的所述业务请求，和/或，所述用户客户端用于确认是否允许所述提供节点向所述使用节点提供所述用户标识对应的用户信用数据；所述第一区块链节点为所述多个区块链节点中的区块链节点。

2、根据权利要求1所述的方法，其特征在于，所述区块链网络中的第一区块链节点
15 发送或者接收通信信息，包括：

所述第一区块链节点向第二区块链节点发送所述通信信息；或者，

所述第一区块链节点接收所述第二区块链节点发送的所述通信信息；或者，

所述第一区块链节点向所述用户客户端发送所述通信信息；或者，

所述第一区块链节点接收所述用户客户端发送的所述通信信息；

20 其中，所述第二区块链节点为所述多个区块链节点中除所述第一区块链节点之外的任一其他区块链节点。

3、根据权利要求1或2所述的方法，其特征在于，所述第一区块链节点为所述使用节点；所述用户客户端用于向所述使用节点发送携带有所述用户标识的所述业务请求；

25 所述区块链网络中的第一区块链节点发送或者接收通信信息，包括：所述使用节点发送或者接收通信信息，其中，所述通信信息具体包括：所述使用节点与所述多个区块链节点中的其他区块链节点之间的信息，以及，所述使用节点与所述用户客户端之间的信息中至少一种。

4、根据权利要求1或2所述的方法，其特征在于，所述第一区块链节点为所述提供节点；所述用户客户端用于确认是否允许所述提供节点向所述使用节点提供所述用户标识对应的用户信用数据；

30 所述区块链网络中的第一区块链节点发送或者接收通信信息，包括：所述提供节点发送或者接收通信信息，其中，所述通信信息具体包括：所述提供节点与所述多个区块链节点中的其他区块链节点之间的信息，以及，所述提供节点与所述用户客户端之间的信息中至少一种。

5、根据权利要求1-3任一所述的方法，其特征在于，所述第一区块链节点为所述使用节点；所述用户客户端用于向所述使用节点发送携带有所述用户标识的所述业务请求；所述区块链网络中的第一区块链节点发送或者接收通信信息，包括以下至少一

种：

所述使用节点接收所述用户客户端发送的携带所述用户标识的所述业务请求；

所述使用节点向所述提供节点发送数据交易请求，所述数据交易请求用于请求获取所述用户标识对应的用户信用数据，所述用户信用数据用于所述使用节点处理携带有所述用户标识的业务请求；

所述使用节点接收所述提供节点发送的数据交易响应，所述数据交易响应包括所述用户标识对应的用户信用数据。

6、根据权利要求1，2或4任一所述的方法，其特征在于，所述第一区块链节点为所述提供节点；所述用户客户端用于确认是否允许所述提供节点向所述使用节点提供所述用户标识对应的用户信用数据；所述区块链网络中的第一区块链节点发送或者接收通信信息，包括以下至少一种：

所述提供节点接收所述使用节点发送的数据交易请求，所述数据交易请求用于请求获取所述用户标识对应的用户信用数据，所述用户信用数据用于所述使用节点处理携带有所述用户标识的业务请求；

所述提供节点向所述用户客户端发送数据授权请求，所述数据授权请求用于请求所述用户客户端允许向所述使用节点提供所述用户标识对应的用户信用数据；

所述提供节点接收所述用户客户端发送的数据授权响应，所述数据授权响应用于确认是否允许向所述使用节点提供所述用户标识对应的用户信用数据；

所述提供节点向所述使用节点发送数据交易响应，所述数据交易响应包括所述用户标识对应的用户信用数据。

7、根据权利要求1或2所述的方法，其特征在于，所述多个区块链节点包括：代理节点；所述代理节点，用于接收所述使用节点发送的数据交易请求，所述数据交易请求用于请求所述用户标识对应的用户信用数据；以及，确认所述使用节点是否具有所述用户标识对应的用户信用数据的访问权限；以及，在确认所述使用节点具有访问权限时，向所述提供节点发送所述数据交易请求；以及，接收所述提供节点发送的数据交易响应，所述数据交易响应包括所述用户标识对应的用户信用数据；

所述第一区块链节点为所述代理节点；所述区块链网络中的第一区块链节点发送或者接收通信信息，包括：所述代理节点发送或者接收通信信息，其中，所述通信信息具体包括：所述代理节点与所述使用节点之间的信息，所述代理节点与所述提供节点之间的信息中至少一种。

8、根据权利要求1-6任一所述的方法，其特征在于，所述区块链网络包括：X个通道；所述区块链网络中的区块链节点分别对应X个通道中的一个或多个通道；其中，所述第一区块链节点对应的通道包括第i通道，所述区块链网络中的第二区块链节点对应的通道包括第i通道；

所述第一区块链节点将所述通信信息记录在区块链网络的账本中，包括：所述第一区块链节点将所述第i通道的通道信息记录在第i通道对应的账本中；

所述第i通道的通道信息包括：所述第一区块链节点与所述第二区块链节点之间通过第i通道传输的信息，以及，所述第一区块链节点或者所述第二区块链节点基于从所述第i通道接收的信息向所述用户客户端发送的信息，以及，所述第一区块链节点基于

从所述用户客户端接收的信息通过第i通道向第二区块链节点发送的信息,以及,所述第二区块链节点基于从所述用户客户端接收的信息通过第i通道向所述第一区块链节点发送的信息中至少一种;

其中, X为大于0的整数, i为大于0且小于或者等于X的整数。

5 9、根据权利要求8所述的方法, 其特征在于, 所述区块链网络包括M个使用节点, M个使用节点分别对应X个通道中的一个通道, 任一使用节点通过自身对应的通道与提供节点传输信息;

所述第一区块链节点为M个使用节点中对应的通道为第i通道的第j个使用节点, 所述第二区块链节点为通过第i通道与第j个使用节点传输信息的提供节点; 或者, 所述
10 所述第一区块链节点为与对应的通道为第i通道的第j个使用节点通过第i通道传输信息的提供节点, 所述第二区块链节点为第j个使用节点;

其中, M为大于0的整数, j为大于0且小于或者等于M的整数。

10、根据权利要求8所述的方法, 其特征在于, 所述区块链网络包括M个使用节点, M个使用节点分别对应X个通道中的一个通道, 任一使用节点通过自身对应的通道与
15 提供节点传输信息;

所述多个区块链节点包括: 代理节点; 所述代理节点, 用于接收所述使用节点发送的数据交易请求, 所述数据交易请求用于请求所述用户标识对应的用户信用数据; 以及, 确认所述使用节点是否具有所述用户标识对应的用户信用数据的访问权限; 以及, 在确认所述使用节点具有访问权限时, 向所述提供节点发送所述数据交易请求;
20 以及, 接收所述提供节点发送的数据交易响应, 所述数据交易响应包括所述用户标识对应的用户信用数据;

所述第一区块链节点为M个使用节点中对应的通道为第i通道的第j个使用节点, 所述第二区块链节点为与第j个使用节点通过第i通道传输信息的代理节点; 或者, 所述
25 所述第一区块链节点为与对应的通道为第i通道的第j个使用节点通过第i通道传输信息的代理节点, 所述第二区块链节点为第j个使用节点; 或者, 所述第一区块链节点为与对应的通道为第i通道的第j个使用节点通过第i通道传输信息的代理节点, 所述第二区块链节点为与所述第一区块链节点通过第i通道传输信息的提供节点;

其中, M为大于0的整数, j为大于0且小于或者等于M的整数。

11、根据权利要求1所述的方法, 其特征在于, 所述提供节点为运营商服务器;
30 所述用户信用数据为所述用户标识对应的运营商信用数据。

12、一种基于区块链网络的数据确权方法, 其特征在于, 所述方法包括:

用户客户端接收提供节点发送的携带有所述用户客户端对应的用户标识的数据授权请求, 所述数据授权请求用于请求允许使用节点使用所述提供节点提供的所述用户标识对应的用户信用数据;

35 所述用户客户端通过自身的输出设备输出提示信息, 所述提示信息用于请求确认是否允许所述使用节点使用所述提供节点提供的所述用户标识对应的用户信用数据;

其中, 所述使用节点、所述提供节点为区块链网络中的区块链节点, 所述使用节点用于向所述提供节点请求所述用户标识对应的用户信用数据。

13、根据权利要求12所述的方法, 其特征在于,

所述用户客户端接收提供节点发送的携带有所述用户客户端对应的用户标识的数据授权请求，包括：所述用户客户端接收至少两个提供节点发送的至少两个数据授权请求，所述至少两个数据授权请求分别与所述至少两个提供节点一一对应，任一数据授权请求用于请求允许所述使用节点使用发送数据授权请求的提供节点提供的所述用户标识对应的用户信用数据；

其中，所述使用节点用于分别向所述至少两个提供节点请求所述用户标识对应的用户信用数据，所述用户标识对应的用户信用数据包括：由所述至少两个提供节点分别提供的所述用户标识对应的用户信用数据；

所述提示信息用于请求确认是否允许所述使用节点使用所述至少两个提供节点分别提供的所述用户标识对应的用户信用数据。

14、根据权利要求13所述的方法，其特征在于，所述方法还包括：

所述用户客户端通过自身的输入设备接收输入信息，所述输入信息用于确认是否允许所述使用节点使用所述至少两个提供节点所提供的所述用户标识对应的用户信用数据；

在所述输入信息表示允许所述使用节点使用所述至少两个提供节点所提供的所述用户标识对应的用户信用数据时，所述用户客户端分别向所述提供节点发送数据授权响应，任一所述数据授权响应用于确认允许所述使用节点使用接收数据授权响应的提供节点所提供的用户标识对应的用户信用数据。

15、根据权利要求12所述的方法，其特征在于，所述数据授权请求用于请求允许所述使用节点在接收到第一业务的业务请求时，使用所述提供节点所提供的所述用户标识对应的用户信用数据。

16、一种基于区块链网络的数据确权系统，其特征在于，所述系统包括：多个区块链节点；所述多个区块链节点包括：使用节点和提供节点；其中，所述使用节点，用于根据携带有用户标识的业务请求，向所述提供节点请求所述用户标识对应的用户信用数据；所述提供节点，用于提供用户信用数据；

所述多个区块链节点中的至少一个区块链节点，还用于发送或者接收通信信息，并将所述通信信息记录在区块链网络的账本中；其中，所述通信信息包括：区块链节点之间的信息，以及，区块链节点与用户客户端之间的信息中至少一种；其中，所述用户客户端用于向所述使用节点发送携带有所述用户标识的所述业务请求，和/或，所述用户客户端用于确认是否允许所述提供节点向所述使用节点提供所述用户标识对应的用户信用数据。

17、根据权利要求16所述的系统，其特征在于，所述至少一个区块链节点为使用节点；所述通信信息具体包括：所述使用节点与所述多个区块链节点中的其他区块链节点之间的信息，以及，所述使用节点与所述用户客户端之间的信息中至少一种；所述用户客户端用于向所述使用节点发送携带有所述用户标识的所述业务请求。

18、根据权利要求16或17所述的系统，其特征在于，所述通信信息具体包括以下至少一种：

所述使用节点接收到的所述用户客户端发送的携带有所述用户标识的业务请求；

所述使用节点向所述提供节点发送的数据交易请求，所述数据交易请求用于请求

获取所述用户标识对应的用户信用数据，所述用户信用数据用于所述使用节点处理携带有所述用户标识的业务请求；

所述使用节点从所述提供节点接收的数据交易响应，所述数据交易响应包括所述用户标识对应的用户信用数据。

5 19、根据权利要求16或17所述的系统，其特征在于，所述至少一个区块链节点为提供节点；所述通信信息具体包括：所述提供节点与所述多个区块链节点中的其他区块链节点之间的信息，以及，所述提供节点与所述用户客户端之间的信息中至少一种；所述用户客户端用于确认是否允许所述提供节点向所述使用节点提供所述用户标识对应的用户信用数据。

10 20、根据权利要求16或19所述的系统，其特征在于，所述通信信息具体包括以下至少一种：

所述提供节点从所述使用节点接收到的数据交易请求，所述数据交易请求用于请求获取所述用户标识对应的用户信用数据，所述用户标识对应的用户信用数据用于所述使用节点处理携带有所述用户标识的业务请求；

15 所述提供节点向所述用户客户端发送的数据授权请求，所述数据授权请求用于请求允许所述使用节点使用所述提供节点所提供的所述用户标识对应的用户信用数据；

所述提供节点从所述用户客户端接收的数据授权响应，所述数据授权响应包括所述用户标识对应的用户信用数据；

20 所述提供节点向所述使用节点发送的数据交易响应，所述数据交易响应包括所述用户标识对应的用户信用数据。

21、根据权利要求16-20任一所述的系统，其特征在于，所述多个区块链节点还包括：代理节点；

25 所述代理节点，用于接收所述使用节点发送的数据交易请求，所述数据交易请求用于请求所述用户标识对应的用户信用数据；以及，确认所述使用节点是否具有所述用户标识对应的用户信用数据的访问权限；以及，在确认所述使用节点具有访问权限时，向所述提供节点发送所述数据交易请求；以及，接收所述提供节点发送的数据交易响应，所述数据交易响应包括所述用户标识对应的用户信用数据；

所述通信信息具体包括：所述代理节点与所述使用节点之间的信息，所述代理节点与所述提供节点之间的信息中至少一种。

30 22、根据权利要求16-20任一所述的系统，其特征在于，所述区块链网络包括：X个通道；所述多个区块链节点分别对应X个通道中的一个或多个通道；其中，

所述使用节点的数量为M个，M个使用节点分别对应X个通道中的一个通道，任一使用节点通过自身对应的通道与提供节点传输信息；

35 所述至少一个区块链节点，具体用于发送或者接收第i通道的通道信息，并将第i通道的通道信息记录在第i通道对应的账本中；

第i通道的通道信息包括以下至少一种：

对应的通道为第i通道的使用节点与第一用户客户端之间的信息，所述第一用户客户端用于向所述使用节点发送携带有所述用户标识的所述业务请求；

对应的通道为第i通道的使用节点与提供节点之间的信息；

提供节点基于从第i通道接收的信息向第二用户客户端发送的信息以及从第二用户客户端接收的信息；所述第二用户客户端用于确认是否允许所述提供节点向所述使用节点提供所述用户标识对应的用户信用数据；

其中，X为大于0的整数，M为大于0的整数，i为大于0且小于或者等于X的整数。

5 23、根据权利要求16所述的系统，其特征在于，所述提供节点，还用于向所述用户客户端发送数据授权请求，所述数据授权请求用于请求允许所述使用节点使用所述提供节点提供的所述用户标识对应的用户信用数据。

24、根据权利要求16所述的系统，其特征在于，所述提供节点为运营商服务器；所述用户信用数据为所述用户标识对应的运营商信用数据。

10 25、一种基于区块链网络的数据确权装置，其特征在于，应用于区块链网络中的第一区块链节点，所述装置包括：

收发模块，用于发送或者接收通信信息；

处理模块，用于将所述通信信息记录在区块链网络的账本中；

15 其中，所述区块链网络包括多个区块链节点，所述多个区块链节点包括：使用节点和提供节点；所述使用节点，用于根据携带有用户标识的业务请求，向所述提供节点请求所述用户标识对应的用户信用数据；所述提供节点，用于向所述使用节点提供用户信用数据；所述通信信息包括：所述第一区块链节点与所述多个区块链节点中的任一其他区块链节点之间的信息，以及，第一区块链节点与用户客户端之间的信息中至少一种；其中，所述用户客户端用于向所述使用节点发送携带有所述用户标识的所述业务请求，和/或，所述用户客户端用于确认是否允许所述提供节点向所述使用节点提供所述用户标识对应的用户信用数据；所述第一区块链节点为所述多个区块链节点中的区块链节点。

26、根据权利要求25所述的装置，其特征在于，所述收发模块，具体用于：

向第二区块链节点发送所述通信信息；或者，

25 接收所述第二区块链节点发送的所述通信信息；或者，

向所述用户客户端发送所述通信信息；或者，

接收所述用户客户端发送的所述通信信息；

其中，所述第二区块链节点为所述多个区块链节点中除所述第一区块链节点之外的任一其他区块链节点。

30 27、根据权利要求25或26所述的装置，其特征在于，所述第一区块链节点为所述使用节点；所述用户客户端用于向所述使用节点发送携带有所述用户标识的所述业务请求；

35 所述收发模块，具体用于发送或者接收通信信息，其中，所述通信信息具体包括：所述使用节点与所述多个区块链节点中的其他区块链节点之间的信息，以及，所述使用节点与所述用户客户端之间的信息中至少一种。

28、根据权利要求25或26所述的装置，其特征在于，所述第一区块链节点为所述提供节点；所述用户客户端用于确认是否允许所述提供节点向所述使用节点提供所述用户标识对应的用户信用数据；

所述收发模块，具体用于发送或者接收通信信息，其中，所述通信信息具体包括：

所述提供节点与所述多个区块链节点中的其他区块链节点之间的信息，以及，所述提供节点与所述用户客户端之间的信息中至少一种。

29、根据权利要求25-27任一所述的装置，其特征在于，所述第一区块链节点为所述使用节点；所述用户客户端用于向所述使用节点发送携带有所述用户标识的所述业务请求；所述收发模块，具体用于以下至少一种：

接收所述用户客户端发送的携带所述用户标识的所述业务请求；

向所述提供节点发送数据交易请求，所述数据交易请求用于请求获取所述用户标识对应的用户信用数据，所述用户信用数据用于所述使用节点处理携带有所述用户标识的业务请求；

接收所述提供节点发送的数据交易响应，所述数据交易响应包括所述用户标识对应的用户信用数据。

30、根据权利要求25，26或28任一所述的装置，其特征在于，所述第一区块链节点为所述提供节点；所述用户客户端用于确认是否允许所述提供节点向所述使用节点提供所述用户标识对应的用户信用数据；所述收发模块，具体用于以下至少一种：

接收所述使用节点发送的数据交易请求，所述数据交易请求用于请求获取所述用户标识对应的用户信用数据，所述用户信用数据用于所述使用节点处理携带有所述用户标识的业务请求；

向所述用户客户端发送数据授权请求，所述数据授权请求用于请求所述用户客户端允许向所述使用节点提供所述用户标识对应的用户信用数据；

接收所述用户客户端发送的数据授权响应，所述数据授权响应用于确认是否允许向所述使用节点提供所述用户标识对应的用户信用数据；

向所述使用节点发送数据交易响应，所述数据交易响应包括所述用户标识对应的用户信用数据。

31、根据权利要求25或26所述的装置，其特征在于，所述多个区块链节点包括：代理节点；所述代理节点，用于接收所述使用节点发送的数据交易请求，所述数据交易请求用于请求所述用户标识对应的用户信用数据；以及，确认所述使用节点是否具有所述用户标识对应的用户信用数据的访问权限；以及，在确认所述使用节点具有访问权限时，向所述提供节点发送所述数据交易请求；以及，接收所述提供节点发送的数据交易响应，所述数据交易响应包括所述用户标识对应的用户信用数据；

所述第一区块链节点为所述代理节点；所述收发模块，具体用于发送或者接收通信信息，其中，所述通信信息具体包括：所述代理节点与所述使用节点之间的信息，所述代理节点与所述提供节点之间的信息中至少一种。

32、根据权利要求25-30任一所述的装置，其特征在于，所述区块链网络包括：X个通道；所述区块链网络中的区块链节点分别对应X个通道中的一个或多个通道；其中，所述第一区块链节点对应的通道包括第i通道，所述区块链网络中的第二区块链节点对应的通道包括第i通道；

所述收发模块，具体用于将所述第i通道的通道信息记录在第i通道对应的账本中；

所述第i通道的通道信息包括：所述第一区块链节点与所述第二区块链节点之间通过第i通道传输的信息，以及，所述第一区块链节点或者所述第二区块链节点基于从所

述第i通道接收的信息向所述用户客户端发送的信息,以及,所述第一区块链节点基于从所述用户客户端接收的信息通过第i通道向第二区块链节点发送的信息,以及,所述第二区块链节点基于从所述用户客户端接收的信息通过第i通道向所述第一区块链节点发送的信息中至少一种;

5 其中,X为大于0的整数,i为大于0且小于或者等于X的整数。

33、根据权利要求32所述的装置,其特征在于,所述区块链网络包括M个使用节点,M个使用节点分别对应X个通道中的一个通道,任一使用节点通过自身对应的通道与提供节点传输信息;

10 所述第一区块链节点为M个使用节点中对应的通道为第i通道的第j个使用节点,所述第二区块链节点为通过第i通道与第j个使用节点传输信息的提供节点;或者,所述第一区块链节点为与对应的通道为第i通道的第j个使用节点通过第i通道传输信息的提供节点,所述第二区块链节点为第j个使用节点;

其中,M为大于0的整数,j为大于0且小于或者等于M的整数。

15 34、根据权利要求32所述的装置,其特征在于,所述区块链网络包括M个使用节点,M个使用节点分别对应X个通道中的一个通道,任一使用节点通过自身对应的通道与提供节点传输信息;

20 所述多个区块链节点包括:代理节点;所述代理节点,用于接收所述使用节点发送的数据交易请求,所述数据交易请求用于请求所述用户标识对应的用户信用数据;以及,确认所述使用节点是否具有所述用户标识对应的用户信用数据的访问权限;以及,在确认所述使用节点具有访问权限时,向所述提供节点发送所述数据交易请求;以及,接收所述提供节点发送的数据交易响应,所述数据交易响应包括所述用户标识对应的用户信用数据;

25 所述第一区块链节点为M个使用节点中对应的通道为第i通道的第j个使用节点,所述第二区块链节点为与第j个使用节点通过第i通道传输信息的代理节点;或者,所述第一区块链节点为与对应的通道为第i通道的第j个使用节点通过第i通道传输信息的代理节点,所述第二区块链节点为第j个使用节点;或者,所述第一区块链节点为与对应的通道为第i通道的第j个使用节点通过第i通道传输信息的代理节点,所述第二区块链节点为与所述第一区块链节点通过第i通道传输信息的提供节点;

其中,M为大于0的整数,j为大于0且小于或者等于M的整数。

30 35、根据权利要求25所述的装置,其特征在于,所述提供节点为运营商服务器;所述用户信用数据为所述用户标识对应的运营商信用数据。

36、一种基于区块链网络的数据确权装置,其特征在于,应用于用户客户端,所述装置包括:

35 收发模块,用于接收提供节点发送的携带有所述用户客户端对应的用户标识的数据授权请求,所述数据授权请求用于请求允许使用节点使用所述提供节点提供的所述用户标识对应的用户信用数据;

输出模块,用于通过输出设备输出提示信息,所述提示信息用于请求确认是否允许所述使用节点使用所述提供节点提供的所述用户标识对应的用户信用数据;

其中,所述使用节点、所述提供节点为区块链网络中的区块链节点,所述使用节

点用于向所述提供节点请求所述用户标识对应的用户信用数据。

37、根据权利要求36所述的装置，其特征在于，

所述收发模块，具体用于接收至少两个提供节点发送的至少两个数据授权请求，所述至少两个数据授权请求分别与所述至少两个提供节点一一对应，任一数据授权请求用于请求允许所述使用节点使用发送数据授权请求的提供节点提供的所述用户标识对应的用户信用数据；

其中，所述使用节点用于分别向所述至少两个提供节点请求所述用户标识对应的用户信用数据，所述用户标识对应的用户信用数据包括：由所述至少两个提供节点分别提供的所述用户标识对应的用户信用数据；

所述提示信息用于请求确认是否允许所述使用节点使用所述至少两个提供节点分别提供的所述用户标识对应的用户信用数据。

38、根据权利要求37所述的装置，其特征在于，所述装置还包括：

输入模块，所述输入模块用于通过输入设备接收输入信息，所述输入信息用于确认是否允许所述使用节点使用所述至少两个提供节点所提供的所述用户标识对应的用户信用数据；

所述收发模块，还用于在所述输入信息表示允许所述使用节点使用所述至少两个提供节点所提供的所述用户标识对应的用户信用数据时，分别向所述提供节点发送数据授权响应，任一所述数据授权响应用于确认允许所述使用节点使用接收数据授权响应的提供节点所提供的用户标识对应的用户信用数据。

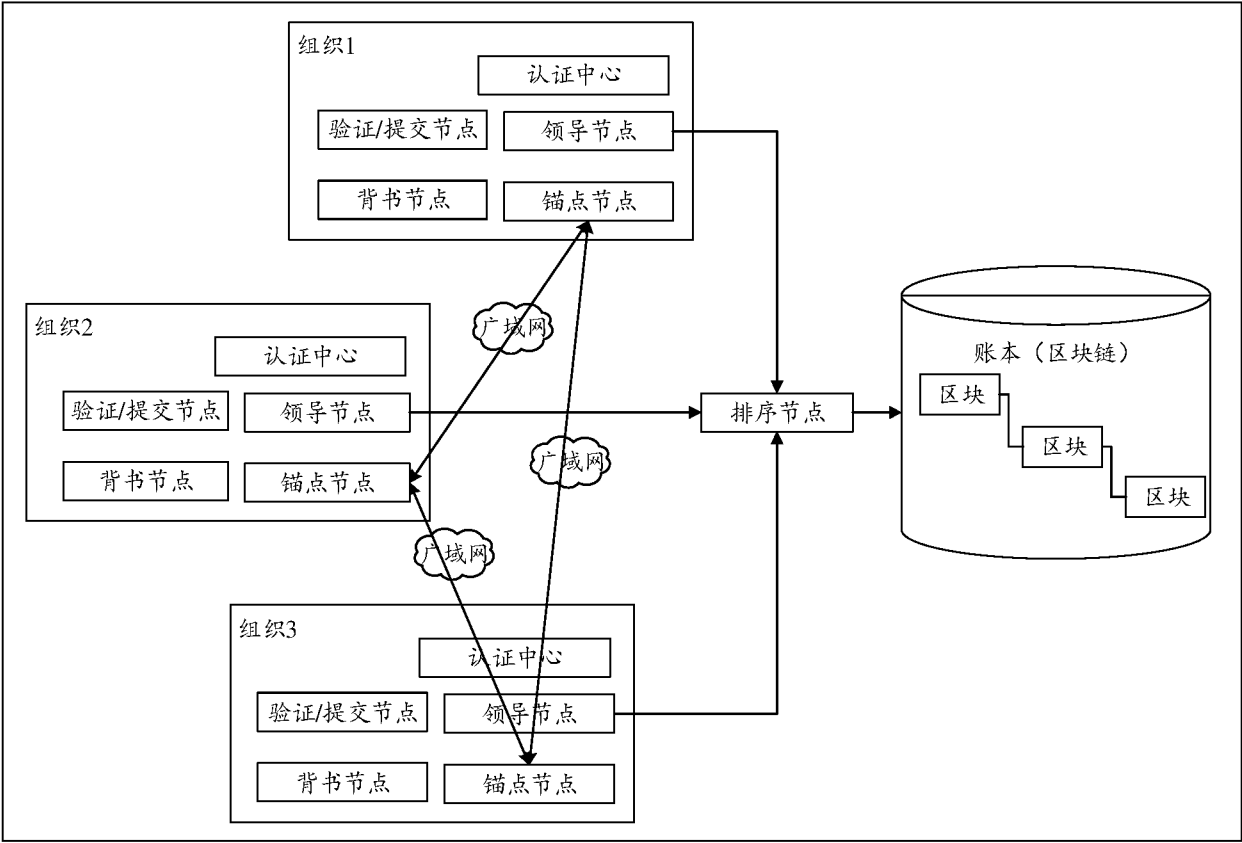


图 1

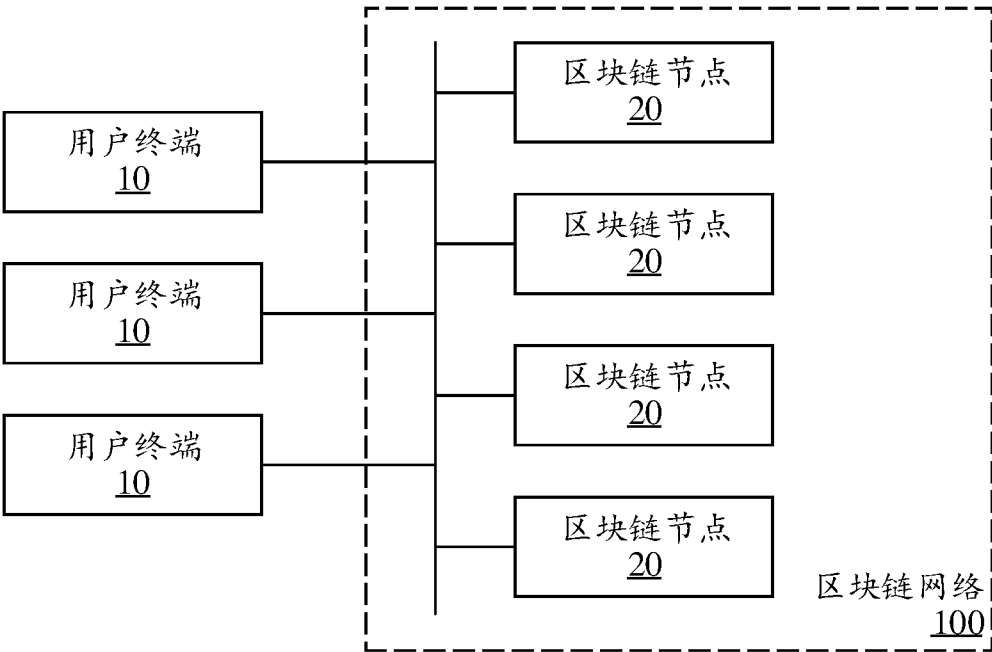


图 2A

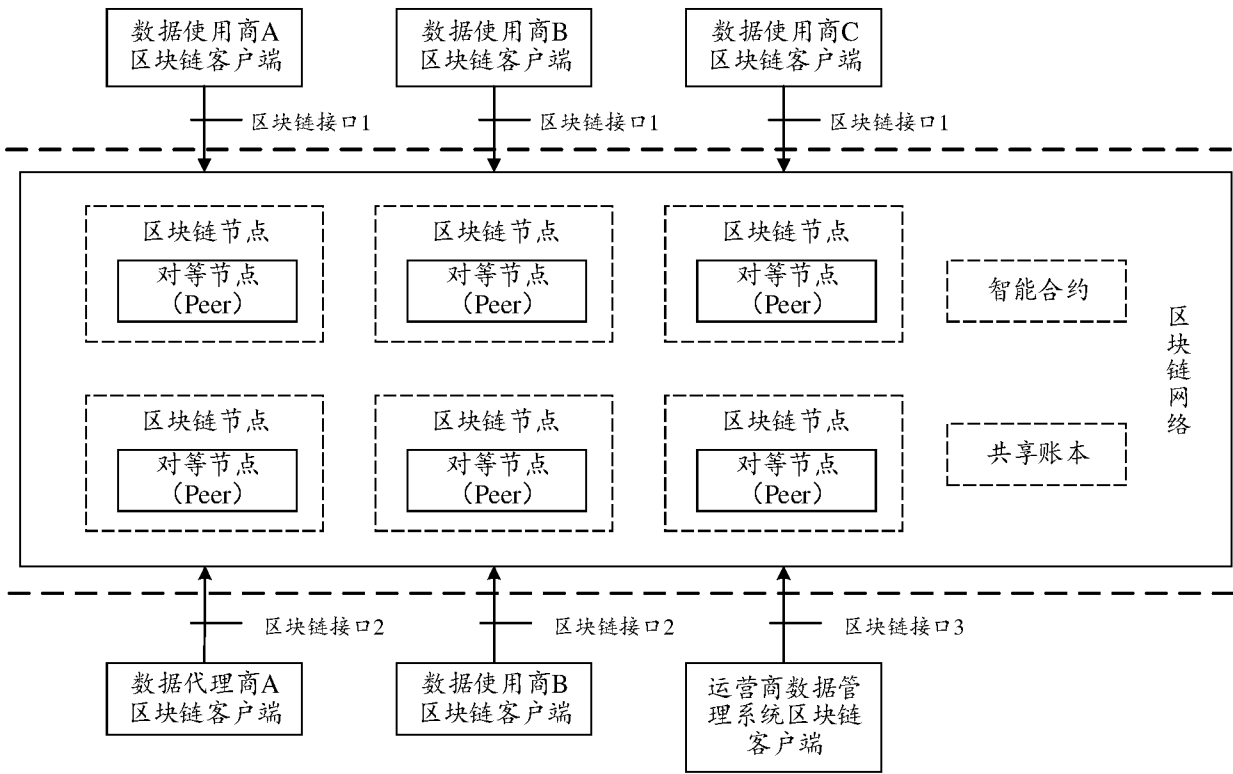


图 2B

3/6

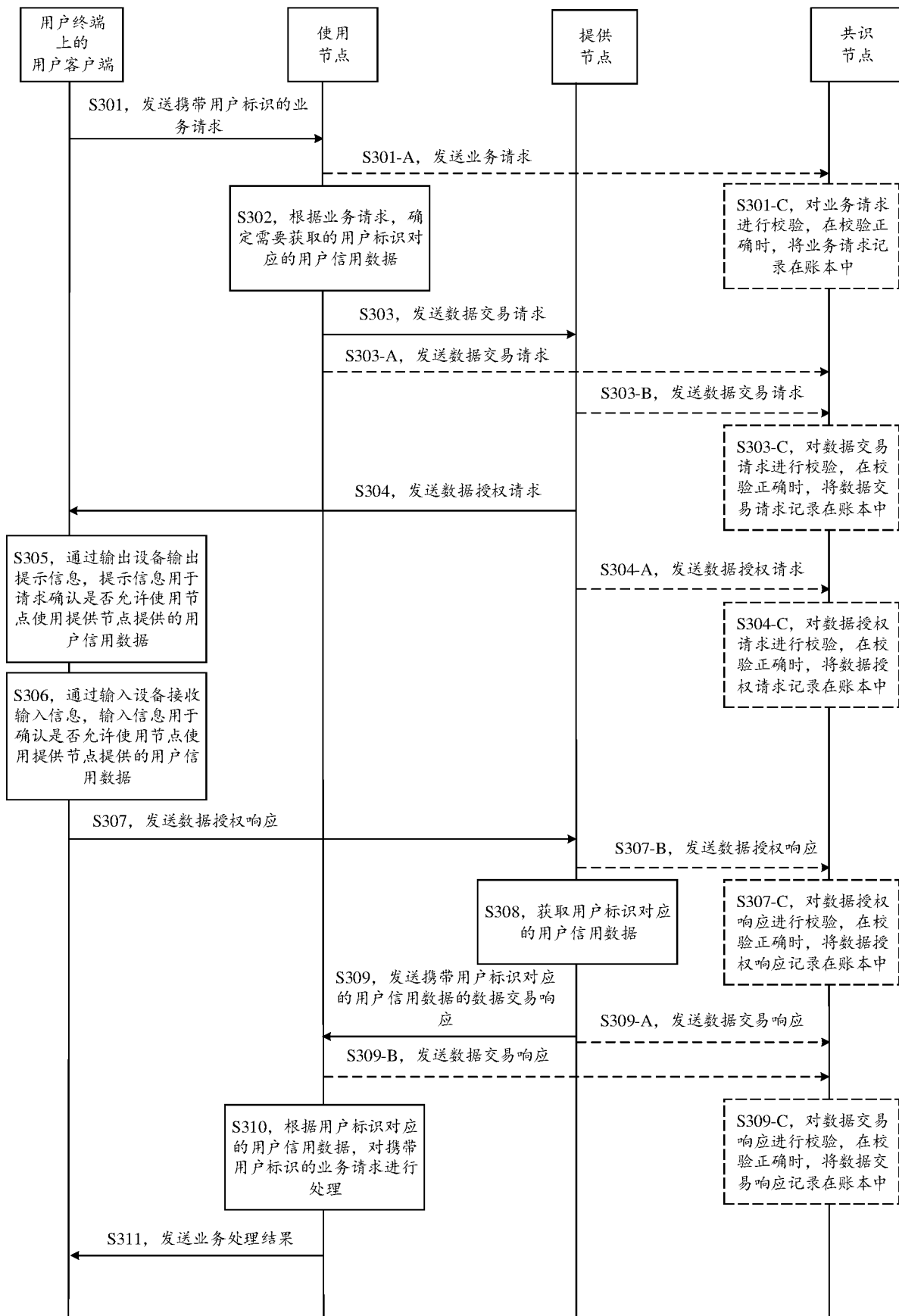


图 3

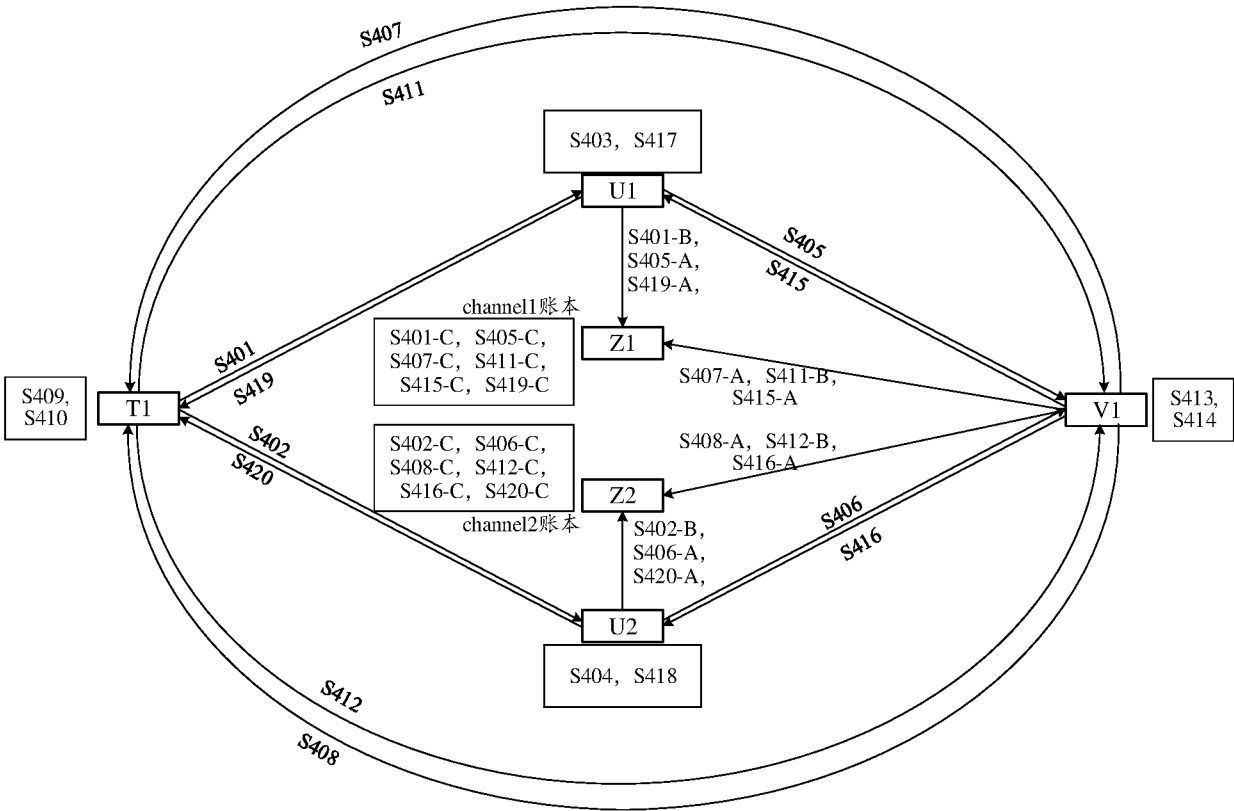


图 4

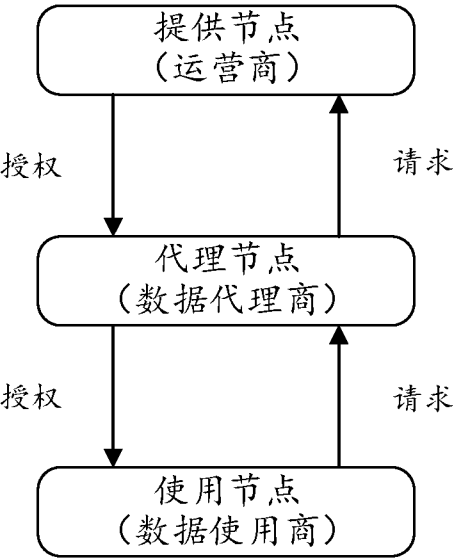


图 5

5/6

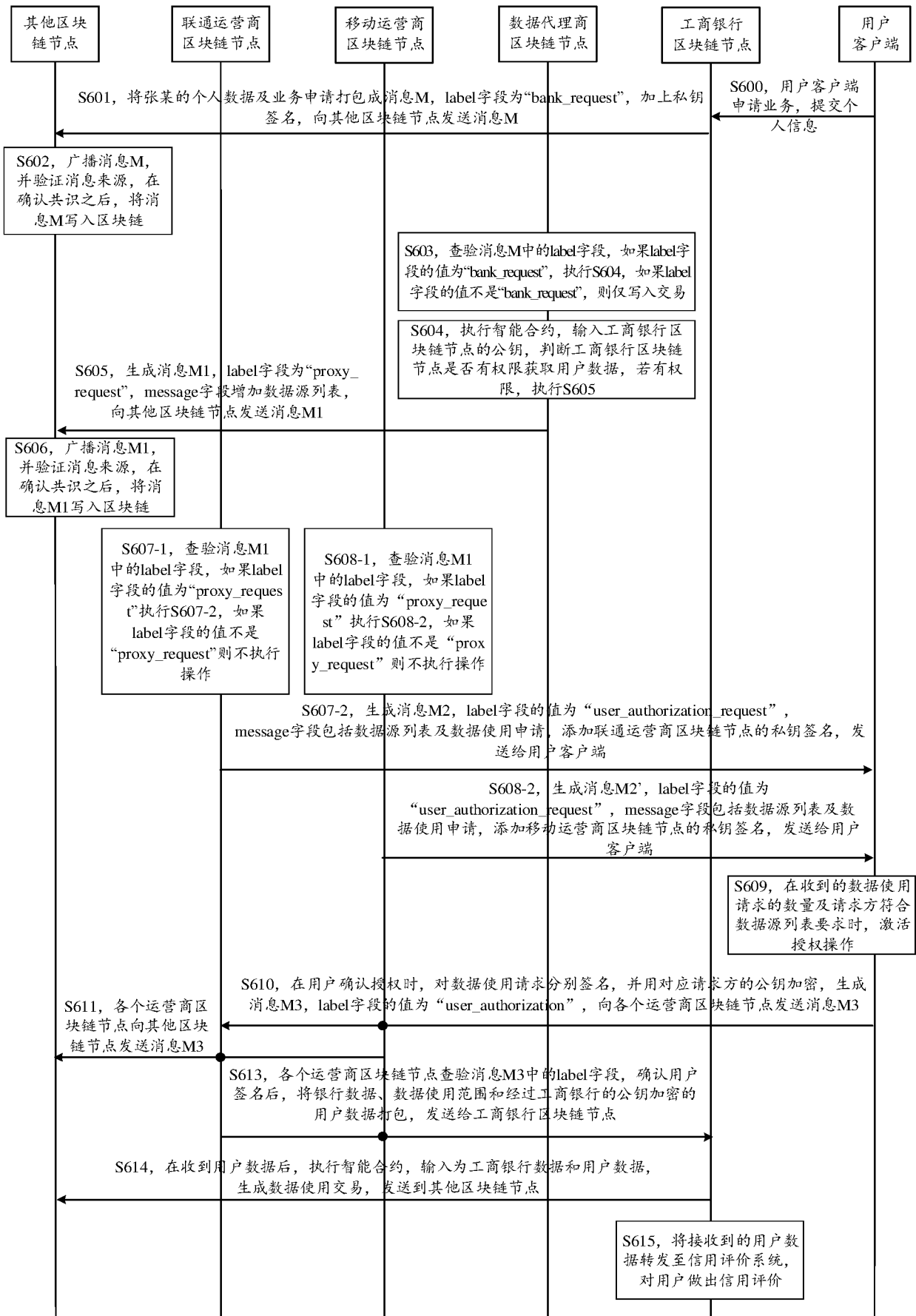


图 6

6/6

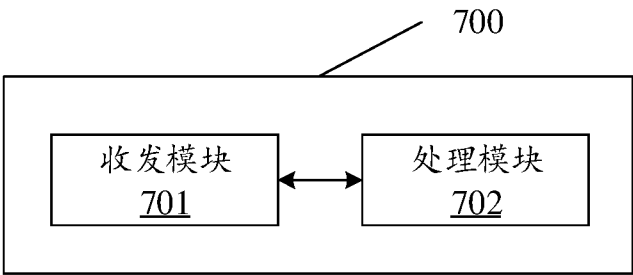


图 7

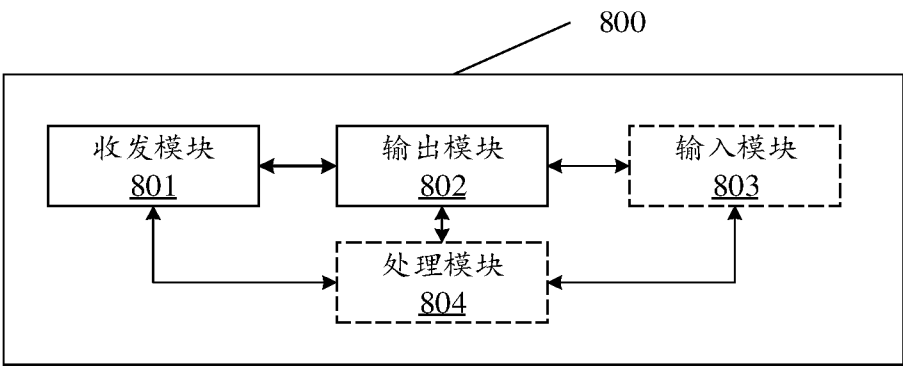


图 8

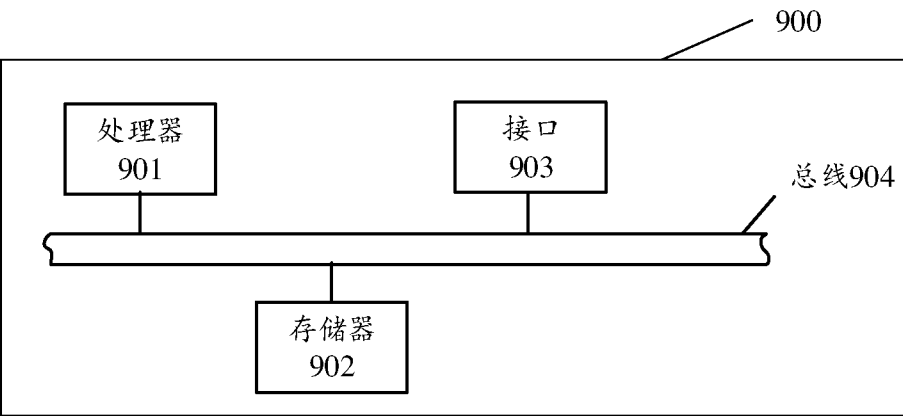


图 9

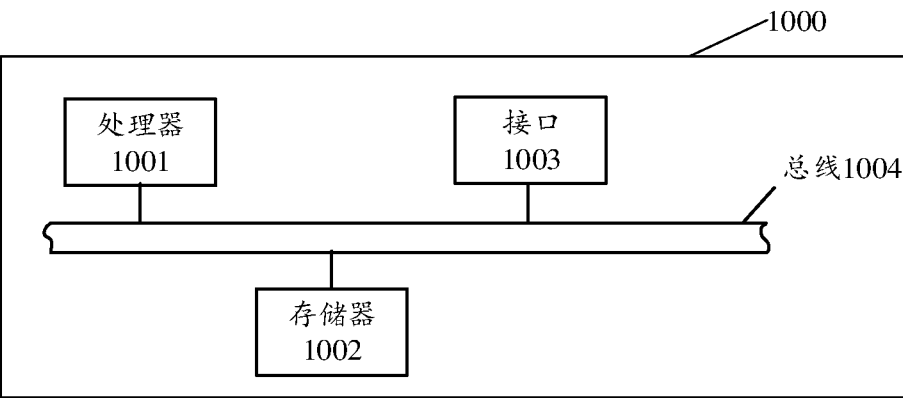


图 10

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2020/080734

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(2006.01)i; H04L 9/32(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)

H04L; G06Q

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

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

CNABS; CNTXT; VEN; USTXT; WOTXT; EPTXT; CNKI; 3GPP; 区块链, 账本, 记账, 写入, 存储, 追溯, 溯源, 追踪, 请求, 信用, 征信, 缴费, 充值, 交易, 记录, 允许, 授权, 同意, 通道, block chain, ledger, account, write, stor+, trace, request, credit, payment, record, allow, authoriz+, channel, grant

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 109544156 A (PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) 29 March 2019 (2019-03-29) description, paragraphs [0037]-[0102]	1-38
Y	CN 109509078 A (PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) 22 March 2019 (2019-03-22) description, paragraphs [0049]-[0079], figure 1	1-11, 16-35
Y	CN 109493093 A (BEIJING BAIDU NETCOM SCIENCE AND TECHNOLOGY CO., LTD.) 19 March 2019 (2019-03-19) description, paragraphs [0088]-[0130]	1-38
A	CN 107833037 A (ALIBABA GROUP HOLDING LIMITED) 23 March 2018 (2018-03-23) entire document	1-38
A	CN 109146478 A (SHANGHAI DIANRONG INFORMATION TECHNOLOGY CO., LTD.) 04 January 2019 (2019-01-04) entire document	1-38
A	US 2019172059 A1 (BANK OF AMERICA) 06 June 2019 (2019-06-06) entire document	1-38



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

13 May 2020

Date of mailing of the international search report

10 June 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/CN2020/080734

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	109544156	A	29 March 2019	None			
CN	109509078	A	22 March 2019	WO	2020056975	A1	26 March 2020
CN	109493093	A	19 March 2019	None			
CN	107833037	A	23 March 2018	TW	201915894	A	16 April 2019
				WO	2019072024	A1	18 April 2019
				HK	1249794	A0	09 November 2018
CN	109146478	A	04 January 2019	None			
US	2019172059	A1	06 June 2019	None			

国际检索报告

国际申请号

PCT/CN2020/080734

A. 主题的分类 H04L 29/06 (2006.01) i; H04L 9/32 (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) H04L; G06Q 包含在检索领域中的除最低限度文献以外的检索文献 在国际检索时查阅的电子数据库 (数据库的名称, 和使用的检索词 (如使用)) CNABS; CNTXT; VEN; USTXT; WOTXT; EPTXT; CNKI; 3GPP: 区块链, 账本, 记账, 写入, 存储, 追溯, 溯源, 追踪, 请求, 信用, 征信, 缴费, 充值, 交易, 记录, 允许, 授权, 同意, 通道, block chain, ledger, account, write, store, trace, request, credit, payment, record, allow, authorize, channel, grant																							
C. 相关文件 <table border="1"> <thead> <tr> <th>类 型*</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>Y</td> <td>CN 109544156 A (平安科技深圳有限公司) 2019年 3月 29日 (2019 - 03 - 29) 说明书第[0037]-[0102]段</td> <td>1-38</td> </tr> <tr> <td>Y</td> <td>CN 109509078 A (平安科技深圳有限公司) 2019年 3月 22日 (2019 - 03 - 22) 说明书第[0049]-[0079]段, 图1</td> <td>1-11, 16-35</td> </tr> <tr> <td>Y</td> <td>CN 109493093 A (百度在线网络技术北京有限公司) 2019年 3月 19日 (2019 - 03 - 19) 说明书第[0088]-[0130]段</td> <td>1-38</td> </tr> <tr> <td>A</td> <td>CN 107833037 A (阿里巴巴集团控股有限公司) 2018年 3月 23日 (2018 - 03 - 23) 全文</td> <td>1-38</td> </tr> <tr> <td>A</td> <td>CN 109146478 A (上海点融信息科技有限责任公司) 2019年 1月 4日 (2019 - 01 - 04) 全文</td> <td>1-38</td> </tr> <tr> <td>A</td> <td>US 2019172059 A1 (BANK OF AMERICA) 2019年 6月 6日 (2019 - 06 - 06) 全文</td> <td>1-38</td> </tr> </tbody> </table>			类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求	Y	CN 109544156 A (平安科技深圳有限公司) 2019年 3月 29日 (2019 - 03 - 29) 说明书第[0037]-[0102]段	1-38	Y	CN 109509078 A (平安科技深圳有限公司) 2019年 3月 22日 (2019 - 03 - 22) 说明书第[0049]-[0079]段, 图1	1-11, 16-35	Y	CN 109493093 A (百度在线网络技术北京有限公司) 2019年 3月 19日 (2019 - 03 - 19) 说明书第[0088]-[0130]段	1-38	A	CN 107833037 A (阿里巴巴集团控股有限公司) 2018年 3月 23日 (2018 - 03 - 23) 全文	1-38	A	CN 109146478 A (上海点融信息科技有限责任公司) 2019年 1月 4日 (2019 - 01 - 04) 全文	1-38	A	US 2019172059 A1 (BANK OF AMERICA) 2019年 6月 6日 (2019 - 06 - 06) 全文	1-38
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求																					
Y	CN 109544156 A (平安科技深圳有限公司) 2019年 3月 29日 (2019 - 03 - 29) 说明书第[0037]-[0102]段	1-38																					
Y	CN 109509078 A (平安科技深圳有限公司) 2019年 3月 22日 (2019 - 03 - 22) 说明书第[0049]-[0079]段, 图1	1-11, 16-35																					
Y	CN 109493093 A (百度在线网络技术北京有限公司) 2019年 3月 19日 (2019 - 03 - 19) 说明书第[0088]-[0130]段	1-38																					
A	CN 107833037 A (阿里巴巴集团控股有限公司) 2018年 3月 23日 (2018 - 03 - 23) 全文	1-38																					
A	CN 109146478 A (上海点融信息科技有限责任公司) 2019年 1月 4日 (2019 - 01 - 04) 全文	1-38																					
A	US 2019172059 A1 (BANK OF AMERICA) 2019年 6月 6日 (2019 - 06 - 06) 全文	1-38																					
☐ 其余文件在C栏的续页中列出。 ☒ 见同族专利附件。																							
<table border="0"> <tr> <td> * 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 </td> <td> “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 </td> </tr> </table>			* 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																			
* 引用文件的具体类型: “A” 认为不特别相关的表示了现有技术一般状态的文件 “E” 在国际申请日的当天或之后公布的在先申请或专利 “L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的) “O” 涉及口头公开、使用、展览或其他方式公开的文件 “P” 公布日先于国际申请日但迟于所要求的优先权日的文件	“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 “X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 “Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 “&” 同族专利的文件																						
国际检索实际完成的日期		国际检索报告邮寄日期																					
2020年 5月 13日		2020年 6月 10日																					
ISA/CN的名称和邮寄地址		受权官员																					
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		吕梅利 电话号码 86-(512)-88996099																					

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2020/080734

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	109544156	A	2019年 3月 29日	无			
CN	109509078	A	2019年 3月 22日	WO	2020056975	A1	2020年 3月 26日
CN	109493093	A	2019年 3月 19日	无			
CN	107833037	A	2018年 3月 23日	TW	201915894	A	2019年 4月 16日
				WO	2019072024	A1	2019年 4月 18日
				HK	1249794	A0	2018年 11月 9日
CN	109146478	A	2019年 1月 4日	无			
US	2019172059	A1	2019年 6月 6日	无			