(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 111553686 A
(43)申请公布日 2020.08.18

(21)申请号 202010353033.X

(22)申请日 2020.04.27

(71)申请人 腾讯科技(深圳)有限公司
地址 518057 广东省深圳市南山区高新区科技中一路腾讯大厦35层

(72)发明人 刘攀

(74)专利代理机构 广州三环专利商标代理有限公司 44202
代理人 熊永强 杜维

(51)Int.Cl.
G06Q 20/38(2012.01)
G06Q 20/02(2012.01)

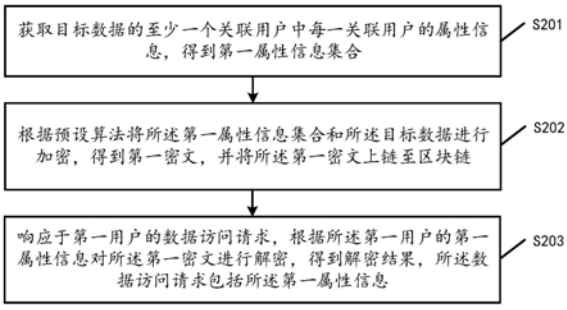
权利要求书2页 说明书11页 附图5页

(54)发明名称

数据处理方法、装置、计算机设备及存储介质

(57)摘要

本发明实施例公开了一种数据处理方法、装置、计算机设备及存储介质,其中方法包括:通过获取目标数据的至少一个关联用户中每一关联用户的属性信息,得到第一属性信息集合;根据预设算法将第一属性信息集合和所述目标数据进行加密,得到第一密文,并将第一密文上链至区块链;进而,在第一用户需要访问目标数据时,响应于第一用户的数据访问请求,根据第一用户的第一属性信息对第一密文进行解密,得到解密结果,所述数据访问请求包括所述第一属性信息,如此,可通过关联用户的属性信息实现数据隔离。



CN 111553686 A

1.一种数据处理方法,其特征在于,所述方法包括:

获取目标数据的至少一个关联用户中每一关联用户的属性信息,得到第一属性信息集合;

根据预设算法将所述第一属性信息集合和所述目标数据进行加密,得到第一密文,并将所述第一密文上链至区块链;

响应于第一用户的数据访问请求,根据所述第一用户的第一属性信息对所述第一密文进行解密,得到解密结果,所述数据访问请求包括所述第一属性信息。

2.根据权利要求1所述方法,其特征在于,所述属性信息包括以下至少一种:用户IP地址、身份信息、访问时间、访问地理位置。

3.根据权利要求1或2所述方法,其特征在于,所述预设算法包括kpabe算法,所述根据预设算法将所述第一属性信息集合和所述目标数据进行加密,得到第一密文,包括:

获取公开参数;

根据所述公开参数对所述目标数据和所述第一属性信息集合进行加密,得到所述第一密文。

4.根据权利要求3所述方法,其特征在于,所述数据访问请求还包括解密秘钥,所述根据所述第一属性信息对所述第一密文进行解密,得到解密结果,包括:

获取解密秘钥;

根据所述解密密钥和所述公开参数对所述第一密文进行解密,得到解密后的所述目标数据和所述第一属性信息集合;

若所述第一属性信息集合包括所述第一属性信息,将所述目标数据对所述第一用户进行授权;

若所述第一属性信息集合不包括所述第一属性信息,提示解密失败。

5.根据权利要求4所述方法,其特征在于,所述获取解密秘钥,包括:

获取访问结构和主密钥;

根据所述访问结构、所述主密钥和所述公开参数生成所述解密密钥。

6.根据权利要求1-5任一项所述方法,其特征在于,所述方法还包括:

获取新增的关联用户,将所述新增的关联用户的属性信息添加至所述第一属性信息集合,得到第二属性信息集合;

根据所述预设算法将所述第二属性信息集合和所述目标数据进行加密,得到第二密文,并将所述第二密文上链至所述区块链。

7.根据权利要求1-6任一项所述方法,其特征在于,所述方法还包括:

将所述第一属性信息集合中的至少一个属性信息进行删除,得到第三属性信息集合;

根据所述预设算法将所述第三属性信息集合和所述目标数据进行加密,得到第三密文,并将所述第三密文上链至所述区块链。

8.一种数据处理装置,其特征在于,所述装置包括:

获取单元,用于获取目标数据的至少一个关联用户中每一关联用户的属性信息,得到第一属性信息集合;

加密单元,用于根据预设算法将所述第一属性信息集合和所述目标数据进行加密,得到第一密文,并将所述第一密文上链至区块链;

解密单元，用于响应于第一用户的数据访问请求，根据所述第一用户的第一属性信息对所述第一密文进行解密，得到解密结果，所述数据访问请求包括所述第一属性信息。

9.一种计算机设备，包括输入设备和输出设备，其特征在于，还包括：

处理器，适于实现一条或一条以上指令；以及，

计算机存储介质，所述计算机存储介质存储有一条或一条以上指令，所述一条或一条以上指令适于由所述处理器加载并执行如权利要求1-7任一项所述的数据处理方法。

10.一种计算机存储介质，其特征在于，所述计算机存储介质存储有一条或一条以上指令，所述一条或一条以上指令适于由处理器加载并执行如权利要求1-7任一项所述的数据处理方法。

数据处理方法、装置、计算机设备及存储介质

技术领域

[0001] 本发明涉及互联网技术领域，具体涉及支付技术领域，尤其涉及一种数据处理方法、装置、计算机设备及存储介质。

背景技术

[0002] 区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。区块链(Blockchain)，本质上是一个去中心化的数据库，是一串使用密码学方法相关联产生的数据块，每一个数据块中包含了一批次网络交易的信息，用于验证其信息的有效性(防伪)和生成下一个区块。

[0003] 区块链具有价值转移、去中心化和不可篡改等特性，区块链可应用于数据交易、金融支付等领域，针对交易数据等需要存储在区块链中的数据，需要对数据进行加密，防止数据泄露，但是，有些数据仅能对部分用户授权访问，因此，如何将数据进行隔离的问题需要解决。

发明内容

[0004] 本发明实施例提供了一种数据处理方法、装置、计算机设备及存储介质，能够通过关联用户的属性信息实现数据隔离，防止数据泄露。

[0005] 一方面，本发明实施例提供了一种数据处理方法，所述方法包括：

[0006] 获取目标数据的至少一个关联用户中每一关联用户的属性信息，得到第一属性信息集合；

[0007] 根据预设算法将所述第一属性信息集合和所述目标数据进行加密，得到第一密文，并将所述第一密文上链至区块链；

[0008] 响应于第一用户的数据访问请求，根据所述第一用户的第一属性信息对所述第一密文进行解密，得到解密结果，所述数据访问请求包括所述第一属性信息。

[0009] 在一个实施例中，所述属性信息包括以下至少一种：用户IP地址、身份信息、访问时间、访问地理位置。

[0010] 在一个实施例中，所述预设算法包括kpabe算法，所述根据预设算法将所述第一属性信息集合和所述目标数据进行加密，得到第一密文，包括：

[0011] 获取公开参数；

[0012] 根据所述公开参数对所述目标数据和所述第一属性信息集合进行加密，得到所述第一密文。

[0013] 在一个实施例中，所述根据所述第一属性信息对所述第一密文进行解密，得到解密结果，包括：

[0014] 获取解密秘钥；

[0015] 根据所述解密密钥和所述公开参数对所述第一密文进行解密，得到解密后的所述目标数据和所述第一属性信息集合；

[0016] 若所述第一属性信息集合包括所述第一属性信息，将所述目标数据对所述第一用户进行授权；

[0017] 若所述第一属性信息集合不包括所述第一属性信息，提示解密失败。

[0018] 在一个实施例中，所述获取解密秘钥，包括：

[0019] 获取访问结构和主密钥；

[0020] 根据所述访问结构、所述主密钥和所述公开参数生成所述解密密钥。

[0021] 在一个实施例中，所述方法还包括：

[0022] 获取新增的关联用户，将所述新增的关联用户的属性信息添加至所述第一属性信息集合，得到第二属性信息集合；

[0023] 根据所述预设算法将所述第二属性信息集合和所述目标数据进行加密，得到第二密文，并将所述第二密文上链至所述区块链。

[0024] 在一个实施例中，所述方法还包括：

[0025] 将所述第一属性信息集合中的至少一个属性信息进行删除，得到第三属性信息集合；

[0026] 根据所述预设算法将所述第三属性信息集合和所述目标数据进行加密，得到第三密文，并将所述第三密文上链至所述区块链。

[0027] 再一方面，本发明实施例提供了一种数据处理装置，所述装置包括：

[0028] 获取单元，用于获取目标数据的至少一个关联用户中每一关联用户的属性信息，得到第一属性信息集合；

[0029] 加密单元，用于根据预设算法将所述第一属性信息集合和所述目标数据进行加密，得到第一密文，并将所述第一密文上链至区块链；

[0030] 解密单元，用于响应于第一用户的数据访问请求，根据所述第一用户的第一属性信息对所述第一密文进行解密，得到解密结果，所述数据访问请求包括所述第一属性信息。

[0031] 在一个实施例中，所述属性信息包括以下至少一种：用户IP地址、身份信息、访问时间、访问地理位置。

[0032] 在一个实施例中，所述预设算法包括kpabe算法，在所述根据预设算法将所述第一属性信息集合和所述目标数据进行加密，得到第一密文方面，所述加密单元，具体用于：

[0033] 获取公开参数；

[0034] 根据所述公开参数对所述目标数据和所述第一属性信息集合进行加密，得到所述第一密文。

[0035] 在一个实施例中，在所述根据所述第一属性信息对所述第一密文进行解密，得到解密结果方面，所述解密单元具体用于：

[0036] 获取解密秘钥；

[0037] 根据所述解密密钥和所述公开参数对所述第一密文进行解密，得到解密后的所述目标数据和所述第一属性信息集合；

[0038] 若所述第一属性信息集合包括所述第一属性信息，将所述目标数据对所述第一用户进行授权；

[0039] 若所述第一属性信息集合不包括所述第一属性信息，提示解密失败。

[0040] 在一个实施例中，在所述获取解密秘钥方面，所述解密单元具体用于：

[0041] 获取访问结构和主密钥；

[0042] 根据所述访问结构、所述主密钥和所述公开参数生成所述解密密钥。

[0043] 在一个实施例中，所述方法还包括：

[0044] 所述获取单元，还用于获取新增的关联用户，将所述新增的关联用户的属性信息添加至所述第一属性信息集合，得到第二属性信息集合；

[0045] 所述加密单元，还用于根据所述预设算法将所述第二属性信息集合和所述目标数据进行加密，得到第二密文，并将所述第二密文上链至所述区块链。

[0046] 在一个实施例中，所述方法还包括：

[0047] 所述获取单元，还用于将所述第一属性信息集合中的至少一个属性信息进行删除，得到第三属性信息集合；

[0048] 所述加密单元，还用于根据所述预设算法将所述第三属性信息集合和所述数据进行加密，得到第三密文，并将所述第三密文上链至所述区块链。

[0049] 再一方面，本发明实施例提供了一种计算机设备，所述计算机设备包括输入设备和输出设备，所述计算机设备还包括：

[0050] 处理器，适于实现一条或一条以上指令；以及，

[0051] 计算机存储介质，所述计算机存储介质存储有一条或一条以上指令，所述一条或一条以上指令适于由所述处理器加载并执行如下步骤：

[0052] 获取目标数据的至少一个关联用户中每一关联用户的属性信息，得到第一属性信息集合；

[0053] 根据预设算法将所述第一属性信息集合和所述目标数据进行加密，得到第一密文，并将所述第一密文上链至区块链；

[0054] 响应于第一用户的数据访问请求，根据所述第一用户的第一属性信息对所述第一密文进行解密，得到解密结果，所述数据访问请求包括所述第一属性信息。

[0055] 再一方面，本发明实施例提供了一种计算机存储介质，所述计算机存储介质存储有一条或一条以上指令，所述一条或一条以上指令适于由处理器加载并执行如下步骤：

[0056] 获取目标数据的至少一个关联用户中每一关联用户的属性信息，得到第一属性信息集合；

[0057] 根据预设算法将所述第一属性信息集合和所述目标数据进行加密，得到第一密文，并将所述第一密文上链至区块链；

[0058] 响应于第一用户的数据访问请求，根据所述第一用户的第一属性信息对所述第一密文进行解密，得到解密结果，所述数据访问请求包括所述第一属性信息。

[0059] 可以看出，本发明实施例，通过获取目标数据的至少一个关联用户中每一关联用户的属性信息，得到第一属性信息集合；根据预设算法将第一属性信息集合和所述目标数据进行加密，得到第一密文，并将第一密文上链至区块链；进而，在第一用户需要访问目标数据时，响应于第一用户的数据访问请求，根据第一用户的第一属性信息对第一密文进行解密，得到解密结果，所述数据访问请求包括所述第一属性信息，如此，可通过关联用户的属性信息实现数据隔离。

附图说明

[0060] 为了更清楚地说明本发明实施例技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0061] 图1a是本发明实施例提供的一种区块链系统的网络架构示意图；

[0062] 图1b是本发明实施例提供的一种区块结构的示意图；

[0063] 图2是本发明实施例提供的一种数据处理方法的流程示意图；

[0064] 图3是本发明实施例提供的另一种数据处理方法的流程示意图；

[0065] 图4是本发明实施例提供的另一种数据处理方法的流程示意图；

[0066] 图5是本发明实施例提供的一种数据处理装置的结构示意图；

[0067] 图6是本发明实施例提供的一种计算机设备的结构示意图；

[0068] 图7是本发明实施例提供的将第一密文、第二密文和第三密文存储在区块链中的示意图。

具体实施方式

[0069] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述。

[0070] 本发明实施例提出一种数据处理方法，该数据处理方法可应用于对需要存储在区块链中的目标数据进行数据隔离的场景，本申请中，以交易数据为例，在产生交易数据后，需要让与交易数据有关的关联用户能够看到交易数据，或者对关联用户进行授权，例如交易业务中的出售方、购买方等用户，因此，可通过本方案的实施步骤，通过关联用户的属性信息，对交易数据进行加密，从而，在关联用户需要查看或者获取交易数据时，可通过自身的属性信息获取或者查看交易数据。而非关联用户的其他人员，则无法查看或者成功获取交易数据，如此，可将交易数据与非关联用户之间进行隔离，防止数据泄露。

[0071] 请参见图1a，是本发明实施例提供的一种区块链系统的网络架构示意图。该区块链系统可以包括终端100和多个计算机设备200，计算机设备可以是服务器或者终端，其中，

[0072] 计算机设备之间形成点对点(P2P，Peer To Peer)网络，P2P协议是一个运行在传输控制协议(TCP，Transmission Control Protocol)协议之上的应用层协议。在区块链系统中，任何机器如服务器、终端都可以加入而成为节点，节点包括硬件层、中间层、操作系统层和应用层。

[0073] 参见图1a示出的区块链系统中各节点的功能，涉及的功能包括：路由、应用和区块链，其中，

[0074] 路由是节点具有的基本功能，用于支持节点之间的通信。

[0075] 节点除具有路由功能外，还可以具有以下功能：

[0076] 应用用于部署在区块链中，根据实际业务需求而实现特定业务，记录实现功能相关的数据形成记录数据，在记录数据中携带数字签名以表示任务数据的来源，将记录数据发送到区块链系统中的其他节点，供其他节点在验证记录数据来源以及完整性成功时，将记录数据添加到临时区块中。例如，应用实现的业务包括：钱包，用于提供进行电子货币的交易的功能，包括发起交易(即，将当前交易的交易记录发送给区块链系统中的其他节点，

其他节点验证成功后，作为承认交易有效的响应，将交易的记录数据存入区块链的临时区块中；当然，钱包还支持查询电子货币地址中剩余的电子货币。共享账本，用于提供账目数据的存储、查询和修改等操作的功能，将对账目数据的操作的记录数据发送到区块链系统中的其他节点，其他节点验证有效后，作为承认账目数据有效的响应，将记录数据存入临时区块中，还可以向发起操作的节点发送确认。智能合约，计算机化的协议，可以执行某个合约的条款，通过部署在共享账本上的用于在满足一定条件时而执行的代码实现，根据实际的业务需求代码用于完成自动化的交易，例如查询买家所购买商品的物流状态，在买家签收货物后将买家的电子货币转移到商户的地址；当然，智能合约不仅限于执行用于交易的合约，还可以执行对接收的信息进行处理的合约。

[0077] 区块链，包括一系列按照产生的先后时间顺序相互接续的区块(Block)，新区块一旦加入到区块链中就不会再被移除，区块中记录了区块链系统中节点提交的记录数据。

[0078] 参见图1b，图1b是本发明实施例提供的区块结构(Block Structure)一个可选的示意图，每个区块中包括本区块存储交易记录的哈希值(本区块的哈希值)、以及前一区块的哈希值，各区块通过哈希值连接形成区块链。另外，区块中还可以包括有区块生成时的时间戳等信息。

[0079] 请参见图2，是本发明实施例提供的一种数据处理方法的流程示意图。如图2所示，该数据处理方法应用于计算机设备，该数据处理方法可以包括以下步骤S201-步骤S203：

[0080] 步骤S201，获取目标数据的至少一个关联用户中每一关联用户的属性信息，得到第一属性信息集合。

[0081] 其中，目标数据为需要存储至区块链中的数据，例如交易数据、应用数据等等。

[0082] 其中，属性信息包括以下至少一种：用户IP地址、身份信息、访问时间、访问地理位置。其中，身份信息可以是用户在数据交易中的身份，例如，出售方、购买方等等，具体实现中，身份信息可包括用户的身份标识码，可通过身份标识码标记关联用户的身份。

[0083] 步骤S202，根据预设算法将所述第一属性信息集合和所述目标数据进行加密，得到第一密文，并将所述第一密文上链至区块链。

[0084] 其中，为了防止目标数据泄露，可通过第一属性信息集合对目标数据和第一属性信息集合中的属性信息进行加密，得到加密后的第一密文，第一密文中包括第一属性信息集合，进而，将第一密文上链至区块链。

[0085] 可选地，所述预设算法包括基于加密的密钥策略属性(key policy attribute based encryption，kpabe)算法，所述根据预设算法将所述第一属性信息集合和所述目标数据进行加密，得到第一密文，包括：

[0086] 获取公开参数；

[0087] 根据所述公开参数对所述目标数据和所述第一属性信息集合进行加密，得到所述第一密文。

[0088] 其中，公开参数可根据如下方式确定：

[0089] 公开参数$PK=(G1,g,g^{y},e(g,g)^{x})$，

[0090] 其中，G1是素数阶P的双线性群，G1的阶是素数P，双线性群G1的生成元是g，随机选取$x,y\in Z_p$，Z_p为数域，x，y均为数域Z_p中的随机数，$e(g,g)^{x}$为对称操作，$e(g,g)^{x}=e(g^{x},g^{x})$。

[0091] 然后，可根据第一属性信息集合和公开参数对目标数据进行加密，得到包括第一属性信息集合的第一密文。从而，可防止目标数据泄露。

[0092] 步骤S203，响应于第一用户的数据访问请求，根据所述第一用户的第一属性信息对所述第一密文进行解密，得到解密结果，所述数据访问请求包括所述第一属性信息。

[0093] 其中，在第一用户需要访问目标数据时，计算机设备可响应于第一用户的数据访问请求，然后，根据第一用户的第一属性信息对第一密文进行解密，若第一用户属于关联用户，则解密成功，可对第一用户授权访问目标数据，若第一用户不属于关联用户，则解密失败，进而，可防止非关联用户获取到目标数据，可将目标数据进行有效隔离。

[0094] 可选地，所述根据所述第一属性信息对所述第一密文进行解密，得到解密结果，包括：

[0095] 获取解密秘钥；

[0096] 根据所述解密密钥和所述公开参数对所述第一密文进行解密，得到解密后的所述目标数据和所述第一属性信息集合；

[0097] 若所述第一属性信息集合包括所述第一属性信息，将所述目标数据对所述第一用户进行授权；

[0098] 若所述第一属性信息集合不包括所述第一属性信息，提示解密失败。

[0099] 其中，可先获取解密秘钥，然后根据解密秘钥和公开参数对第一密文进行解密，得到目标数据和第一属性信息集合的明文，若第一属性信息集合包括第一属性信息，表明第一用户为关联用户，进而，可将所述目标数据对所述第一用户进行授权。若第一属性信息集合不包括第一属性信息，表明第一用户不属于关联用户，进而，可提示解密失败。

[0100] 可选地，所述获取解密秘钥，包括：

[0101] 获取访问结构和主密钥；

[0102] 根据所述访问结构、所述主密钥和所述公开参数生成所述解密密钥。

[0103] 其中，计算机设备可自身设置访问结构，进而，可根据访问结构、主密钥、公开参数和秘钥生成算法生成解密密钥。

[0104] 可选地，获取解密秘钥，可以接收第一用户通过终端发送的解密秘钥，具体实现中，计算机设备可接收携带解密秘钥的数据访问请求，其中，解密秘钥可以是终端根据访问结构、主密钥和公开参数，以及预设的秘钥生成算法生成的秘钥。

[0105] 可选地，所述方法还包括：

[0106] 获取新增的关联用户，将所述新增的关联用户的属性信息添加至所述第一属性信息集合，得到第二属性信息集合；

[0107] 根据所述预设算法将所述第二属性信息集合和所述目标数据进行加密，得到第二密文，并将所述第二密文上链至所述区块链。

[0108] 其中，若需要在原来的至少一个关联用户的基础上增加新的关联用户，可将新增的关联用户的属性信息添加至第一属性信息集合，得到第二属性信息集合，然后将第二属性信息集合和目标数据进行加密，得到第二密文，第二密文为与第一密文独立的新的密文，进而，若有第二用户需要访问目标数据，可将第二用户的第二用户属性和第二属性信息集合对第二密文进行解密。

[0109] 可选地，所述方法还包括：

[0110] 将所述第一属性信息集合中的至少一个属性信息进行删除，得到第三属性信息集合；

[0111] 根据所述预设算法将所述第三属性信息集合和所述目标数据进行加密，得到第三密文，并将所述第三密文上链至所述区块链。

[0112] 其中，若需要在原来的至少一个关联用户的基础上减少关联用户，可将第一属性信息集合中的至少一个属性信息进行删除，得到第三属性信息集合，然后将第三属性信息集合和目标数据进行加密，得到第三密文，第三密文为与第一密文、第二密文独立的新的密文，进而，若有第三用户需要访问目标数据，可将第三用户的第三用户属性和第三属性信息集合对第三密文进行解密。

[0113] 本发明实施例通过获取目标数据的至少一个关联用户中每一关联用户的属性信息，得到第一属性信息集合；根据预设算法将第一属性信息集合和所述目标数据进行加密，得到第一密文，并将第一密文上链至区块链；进而，在第一用户需要访问目标数据时，响应于第一用户的数据访问请求，根据第一用户的第一属性信息对第一密文进行解密，得到解密结果，所述数据访问请求包括所述第一属性信息，如此，可通过关联用户的属性信息实现数据隔离。

[0114] 进一步的，请参见图3，是本发明实施例提供的另一种数据处理方法的流程示意图。上述数据处理方法应用于计算机设备，如图3所示，上述数据处理方法可以包括：

[0115] 步骤S301，获取目标数据的至少一个关联用户中每一关联用户的属性信息，得到第一属性信息集合。

[0116] 步骤S302，获取公开参数。

[0117] 步骤S303，根据所述公开参数对所述目标数据和所述第一属性信息集合进行加密，得到所述第一密文，将所述第一密文上链至区块链。

[0118] 步骤S304，响应于第一用户的数据访问请求，根据所述解密密钥和所述公开参数对所述第一密文进行解密，得到解密后的所述目标数据和所述第一属性信息集合，所述数据访问请求包括第一属性信息和所述解密秘钥。

[0119] 步骤S305，若所述第一属性信息集合包括所述第一属性信息，将所述目标数据对所述第一用户进行授权。

[0120] 步骤S306，若所述第一属性信息集合不包括所述第一属性信息，提示解密失败。

[0121] 举例说明，在网络交易场景下产生的交易数据，可通过本申请实施例的步骤进行数据隔离，具体地，计算机设备可获取需要授予权限的交易数据至少一个关联用户的属性信息，得到第一属性信息集合，然后，获取公开参数，根据公开参数对交易数据和第一属性信息集合进行加密，得到第一密文，从而，可避免交易数据泄露。在第一用户需要访问交易数据时，可向计算机设备发送数据访问请求，然后计算机设备获取数据访问请求后，可根据数据访问请求对第一密文进行解密，得到解密后的目标数据和第一属性信息集合，若第一属性信息集合包括第一属性信息，将交易数据对第一用户进行授权，从而，第一用户可查看交易数据，若第一属性信息集合不包括第一属性信息，提示解密失败，可提示解密失败。

[0122] 本发明实施例通过获取目标数据的至少一个关联用户中每一关联用户的属性信息，得到第一属性信息集合；根据kpabe算法将第一属性信息集合和所述目标数据进行加密，得到第一密文，并将第一密文上链至区块链；进而，在第一用户需要访问目标数据时，响

应于第一用户的数据访问请求，根据第一用户的第一属性信息对第一密文进行解密，得到解密结果，所述数据访问请求包括所述第一属性信息，如此，可通过关联用户的属性信息实现数据隔离，提高数据安全性。

[0123] 请参见图4，是本发明实施例提供的一种数据处理方法的流程示意图。如图4所示，该数据处理方法应用于计算机设备和终端，该数据处理方法可以包括以下步骤S401-步骤S402：

[0124] 步骤S401，计算机设备获取目标数据的至少一个关联用户中每一关联用户的属性信息，得到第一属性信息集合。

[0125] 步骤S402，计算机设备根据预设算法将所述第一属性信息集合和所述目标数据进行加密，得到第一密文，并将所述第一密文上链至区块链。

[0126] 步骤S403，终端向计算机设备发送第一用户的数据访问请求，所述数据访问请求包括所述第一属性信息。

[0127] 具体实施中，终端可设置访问结构，获取主密钥和公开参数，然后根据访问结构、主密钥和公开参数生成解密密钥，然后向计算机设备发送携带第一用户的第一属性信息和解密秘钥的数据访问请求。

[0128] 步骤S404，响应于第一用户的数据访问请求，根据所述第一用户的第一属性信息对所述第一密文进行解密，得到解密结果。

[0129] 其中，计算机设备接收到数据访问请求后，可根据解密秘钥和公开参数对第一密文进行解密，得到解密后的目标数据和第一属性信息集合。

[0130] 步骤S405，向终端反馈所述解密结果。

[0131] 其中，若第一属性信息集合包括所述第一属性信息，将所述目标数据对所述第一用户进行授权，向终端反馈目标数据。若所述第一属性信息集合不包括所述第一属性信息，向终端反馈解密失败的信息，以提示解密失败。

[0132] 本发明实施例通过获取目标数据的至少一个关联用户中每一关联用户的属性信息，得到第一属性信息集合；根据预设算法将第一属性信息集合和所述目标数据进行加密，得到第一密文，并将第一密文上链至区块链；进而，在第一用户需要访问目标数据时，响应于第一用户的数据访问请求，根据第一用户的第一属性信息对第一密文进行解密，得到解密结果，所述数据访问请求包括所述第一属性信息，如此，可通过关联用户的属性信息实现数据隔离，提高数据安全性。

[0133] 进一步的，请参见图5，是本发明实施例提供的一种数据处理装置600的结构示意图。如图5所示，所述数据处理装置500应用于计算机设备，所述数据处理装置500可以包括：获取单元501、加密单元502和解密单元503；其中，

[0134] 所述获取单元501，用于获取目标数据的至少一个关联用户中每一关联用户的属性信息，得到第一属性信息集合；

[0135] 所述加密单元502，用于根据预设算法将所述第一属性信息集合和所述目标数据进行加密，得到第一密文，并将所述第一密文上链至区块链；

[0136] 所述解密单元503，用于响应于第一用户的数据访问请求，根据所述第一用户的第一属性信息对所述第一密文进行解密，得到解密结果，所述数据访问请求包括所述第一属性信息。

[0137] 其中，获取单元501、加密单元502和解密单元503的具体功能实现方式可以参见上述图2对应实施例中的步骤S201-步骤S203，这里不再进行赘述。

[0138] 在一个实施例中，所述属性信息包括以下至少一种：用户IP地址、身份信息、访问时间、访问地理位置。

[0139] 在一个实施例中，所述预设算法包括kpabe算法，在所述根据预设算法将所述第一属性信息集合和所述目标数据进行加密，得到第一密文方面，所述加密单元502，具体用于：

[0140] 获取公开参数；

[0141] 根据所述公开参数对所述目标数据和所述第一属性信息集合进行加密，得到所述第一密文。

[0142] 在一个实施例中，在所述根据所述第一属性信息对所述第一密文进行解密，得到解密结果方面，所述解密单元503具体用于：

[0143] 获取解密秘钥；

[0144] 根据所述解密密钥和所述公开参数对所述第一密文进行解密，得到解密后的所述目标数据和所述第一属性信息集合；

[0145] 若所述第一属性信息集合包括所述第一属性信息，将所述目标数据对所述第一用户进行授权；

[0146] 若所述第一属性信息集合不包括所述第一属性信息，提示解密失败。

[0147] 在一个实施例中，在所述获取解密秘钥方面，所述解密单元503具体用于：

[0148] 获取访问结构和主密钥；

[0149] 根据所述访问结构、所述主密钥和所述公开参数生成所述解密密钥。

[0150] 在一个实施例中，所述方法还包括：

[0151] 所述获取单元501，还用于获取新增的关联用户，将所述新增的关联用户的属性信息添加至所述第一属性信息集合，得到第二属性信息集合；

[0152] 所述加密单元502，还用于根据所述预设算法将所述第二属性信息集合和所述目标数据进行加密，得到第二密文，并将所述第二密文上链至所述区块链。

[0153] 在一个实施例中，所述方法还包括：

[0154] 所述获取单元501，还用于将所述第一属性信息集合中的至少一个属性信息进行删除，得到第三属性信息集合；

[0155] 所述加密单元502，还用于根据所述预设算法将所述第三属性信息集合和所述数据进行加密，得到第三密文，并将所述第三密文上链至所述区块链。

[0156] 可以看出，本发明实施例提供的数据处理装置，通过获取目标数据的至少一个关联用户中每一关联用户的属性信息，得到第一属性信息集合；根据预设算法将第一属性信息集合和所述目标数据进行加密，得到第一密文，并将第一密文上链至区块链；进而，在第一用户需要访问目标数据时，响应于第一用户的数据访问请求，根据第一用户的第一属性信息对第一密文进行解密，得到解密结果，所述数据访问请求包括所述第一属性信息，如此，可通过关联用户的属性信息实现数据隔离，提高数据安全性。

[0157] 根据本发明的另一个实施例，图5所示的数据处理装置中的各个单元可以分别或全部合并为一个或若干个另外的单元来构成，或者其中的某个(些)单元还可以再拆分为功能上更小的至少两个单元来构成，这可以实现同样的操作，而不影响本发明的实施例的技

术效果的实现。上述单元是基于逻辑功能划分的，在实际应用中，一个单元的功能也可以由至少两个单元来实现，或者至少两个单元的功能由一个单元实现。在本发明的其它实施例中，基于数据处理装置也可以包括其它单元，在实际应用中，这些功能也可以由其它单元协助实现，并且可以由至少两个单元协作实现。

[0158] 进一步地，请参见图6，是本发明实施例提供的一种计算机设备的结构示意图。如图6所示，上述图6中的数据处理装置600可以应用于所述计算机设备6000，所述计算机设备6000可以包括：处理器6001，网络接口6004和存储器6005，此外，所述计算机设备6000还可以包括：用户接口6003，和至少一个通信总线6002。其中，通信总线6002用于实现这些组件之间的连接通信。其中，用户接口6003可以包括标准的有线接口、无线接口。网络接口6004可选的可以包括标准的有线接口、无线接口(如WI-FI接口)。存储器6004可以是高速RAM存储器，也可以是非不稳定的存储器(non-volatile memory)，例如至少一个磁盘存储器。存储器6004可选的还可以是至少一个位于远离前述处理器6001的存储装置。如图6所示，作为一种计算机存储介质的存储器6004中可以包括操作系统、网络通信模块、用户接口模块以及设备控制应用程序。

[0159] 在图6所示的计算机设备6000中，网络接口6004可提供网络通讯功能；而用户接口6003主要用于为用户提供输入的接口；而处理器6001可以用于调用存储器6004中存储的设备控制应用程序，以实现：

[0160] 获取目标数据的至少一个关联用户中每一关联用户的属性信息，得到第一属性信息集合；

[0161] 根据预设算法将所述第一属性信息集合和所述目标数据进行加密，得到第一密文，并将所述第一密文上链至区块链；

[0162] 响应于第一用户的数据访问请求，根据所述第一用户的第一属性信息对所述第一密文进行解密，得到解密结果，所述数据访问请求包括所述第一属性信息。

[0163] 在一个实施例中，所述属性信息包括以下至少一种：用户IP地址、身份信息、访问时间、访问地理位置。

[0164] 在一个实施例中，所述预设算法包括kpabe算法，在所述根据预设算法将所述第一属性信息集合和所述目标数据进行加密，得到第一密文方面，所述处理器6001具体执行以下步骤：

[0165] 获取公开参数；

[0166] 根据所述公开参数对所述目标数据和所述第一属性信息集合进行加密，得到所述第一密文。

[0167] 在一个实施例中，所述数据访问请求还包括解密秘钥，在所述根据所述第一属性信息对所述第一密文进行解密，得到解密结果方面，所述处理器6001具体执行以下步骤：

[0168] 获取解密秘钥；

[0169] 根据所述解密密钥和所述公开参数对所述第一密文进行解密，得到解密后的所述目标数据和所述第一属性信息集合；

[0170] 若所述第一属性信息集合包括所述第一属性信息，将所述目标数据对所述第一用户进行授权；

[0171] 若所述第一属性信息集合不包括所述第一属性信息，提示解密失败。

[0172] 在一个实施例中，在所述获取解密秘钥方面，所述处理器6001具体执行以下步骤：

[0173] 获取访问结构和主密钥；

[0174] 根据所述访问结构、所述主密钥和所述公开参数生成所述解密密钥。

[0175] 在一个实施例中，所述处理器6001还具体执行以下步骤：

[0176] 获取新增的关联用户，将所述新增的关联用户的属性信息添加至所述第一属性信息集合，得到第二属性信息集合；

[0177] 根据所述预设算法将所述第二属性信息集合和所述目标数据进行加密，得到第二密文，并将所述第二密文上链至所述区块链。

[0178] 在一个实施例中，所述处理器6001还具体执行以下步骤：

[0179] 将所述第一属性信息集合中的至少一个属性信息进行删除，得到第三属性信息集合；

[0180] 根据所述预设算法将所述第三属性信息集合和所述目标数据进行加密，得到第三密文，并将所述第三密文上链至所述区块链。

[0181] 应当理解，本发明实施例中所描述的计算机设备6000可执行前文图2和图3所对应实施例中对所述数据处理方法的描述，也可执行前文图5所对应实施例中对所述数据处理装置的描述，在此不再赘述。另外，对采用相同方法的有益效果描述，也不再进行赘述。

[0182] 本发明实施例还提供了一种计算机存储介质，且所述计算机存储介质中存储有前文提及的计算机设备6000所执行的计算机程序，且所述计算机程序包括程序指令，当所述处理器执行所述程序指令时，能够执行前文图2实施例中对所述多媒体数据处理方法的描述，因此，这里将不再进行赘述。另外，对采用相同方法的有益效果描述，也不再进行赘述。对于本发明所涉及的计算机存储介质实施例中未披露的技术细节，请参照本发明方法实施例的描述。

[0183] 请参见图7，图7是本发明实施例提供的区块结构(Block Structure)另一个可选的示意图，每个区块中包括本区块存储交易记录的哈希值(本区块的哈希值)、以及前一区块的哈希值，各区块通过哈希值连接形成区块链，本发明实施例中，可将生成的第一密文、第二密文和第三密文存储在上述区块链中，上述第一密文、第二密文和第三密文可分别存储在区块链中不同的多个区块中。

[0184] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，是可以通过计算机程序来指令相关的硬件来完成，所述的程序可存储于一计算机可读取存储介质中，该程序在执行时，可包括如上述各方法的实施例的流程。其中，所述的存储介质可为磁碟、光盘、只读存储记忆体(Read-Only Memory，ROM)或随机存储记忆体(Random Access Memory，RAM)等。

[0185] 以上所揭露的仅为本发明较佳实施例而已，当然不能以此来限定本发明之权利范围，因此依本发明权利要求所作的等同变化，仍属本发明所涵盖的范围。

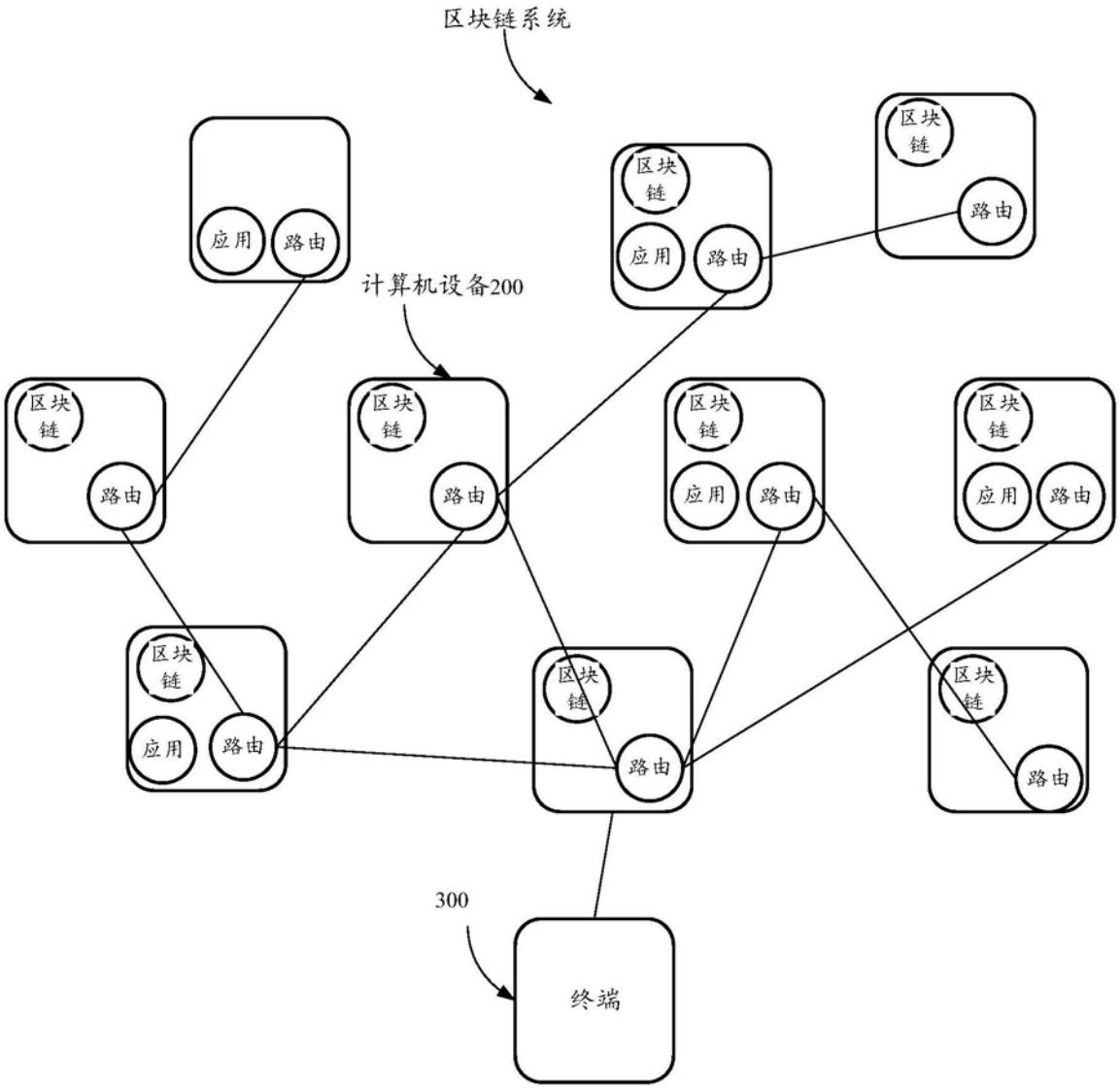

区块链系统
应用
路由
计算机设备200
区块链
路由
区块链
应用
路由
区块链
路由
区块链
路由
区块链
应用
路由
区块链
应用
路由
区块链
应用
路由
区块链
路由
区块链
路由
300
终端

图1a

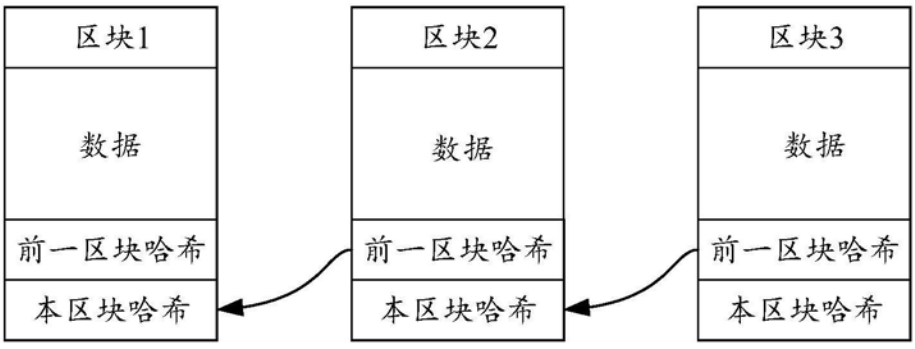

区块1
数据
前一区块哈希
本区块哈希
区块2
数据
前一区块哈希
本区块哈希
区块3
数据
前一区块哈希
本区块哈希

图1b

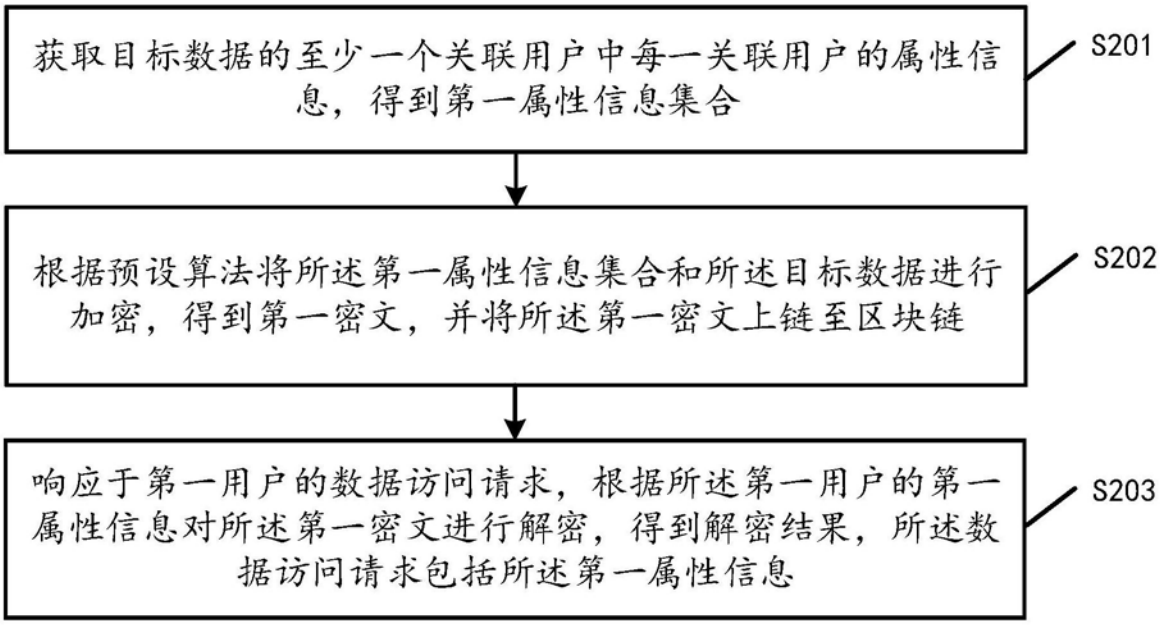

获取目标数据的至少一个关联用户中每一关联用户的属性信息，得到第一属性信息集合
S201
根据预设算法将所述第一属性信息集合和所述目标数据进行加密，得到第一密文，并将所述第一密文上链至区块链
S202
响应于第一用户的数据访问请求，根据所述第一用户的第一属性信息对所述第一密文进行解密，得到解密结果，所述数据访问请求包括所述第一属性信息
S203

图2

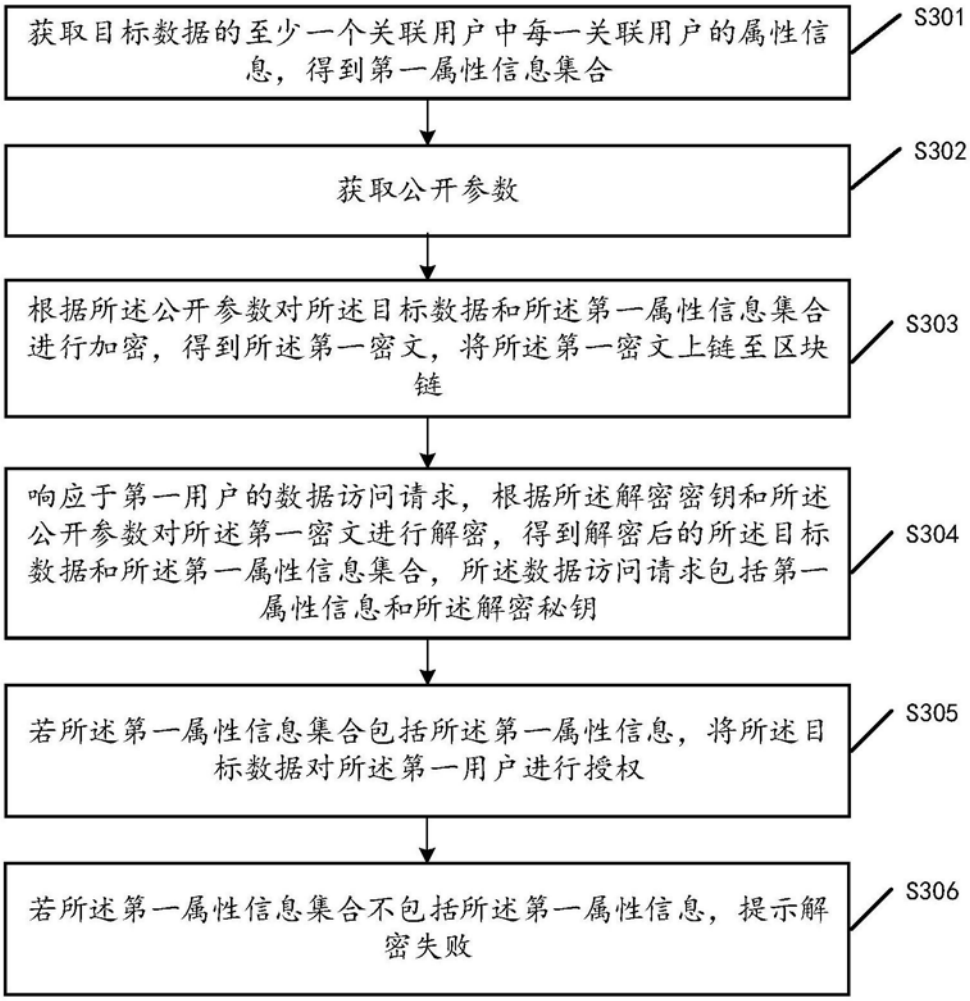

获取目标数据的至少一个关联用户中每一关联用户的属性信息，得到第一属性信息集合
S301
获取公开参数
S302
根据所述公开参数对所述目标数据和所述第一属性信息集合进行加密，得到所述第一密文，将所述第一密文上链至区块链
S303
响应于第一用户的数据访问请求，根据所述解密密钥和所述公开参数对所述第一密文进行解密，得到解密后的所述目标数据和所述第一属性信息集合，所述数据访问请求包括第一属性信息和所述解密秘钥
S304
若所述第一属性信息集合包括所述第一属性信息，将所述目标数据对所述第一用户进行授权
S305
若所述第一属性信息集合不包括所述第一属性信息，提示解密失败
S306

图3

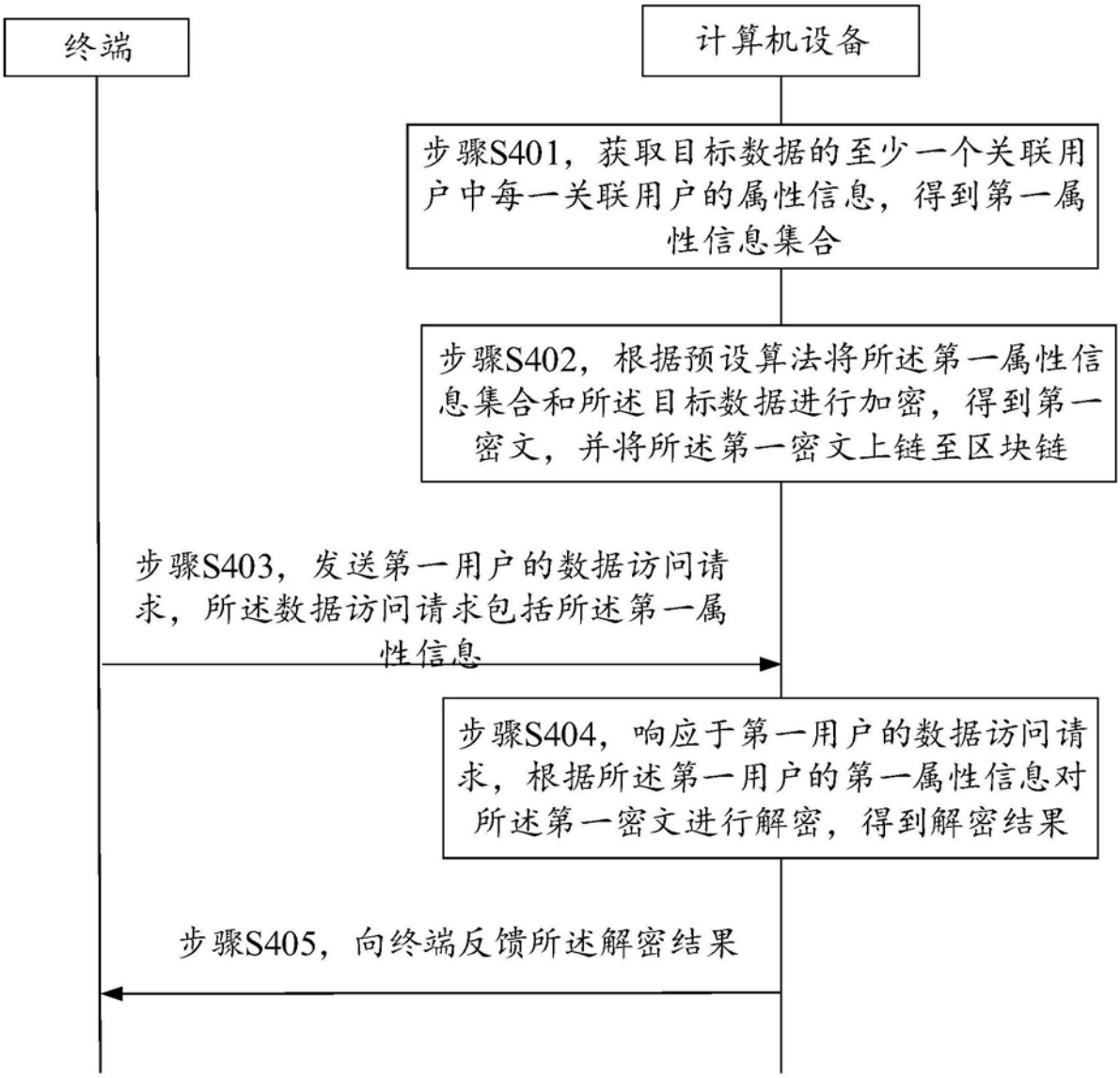

终端
计算机设备
步骤S401，获取目标数据的至少一个关联用户中每一关联用户的属性信息，得到第一属性信息集合
步骤S402，根据预设算法将所述第一属性信息集合和所述目标数据进行加密，得到第一密文，并将所述第一密文上链至区块链
步骤S403，发送第一用户的数据访问请求，所述数据访问请求包括所述第一属性信息
步骤S404，响应于第一用户的数据访问请求，根据所述第一用户的第一属性信息对所述第一密文进行解密，得到解密结果
步骤S405，向终端反馈所述解密结果

图4

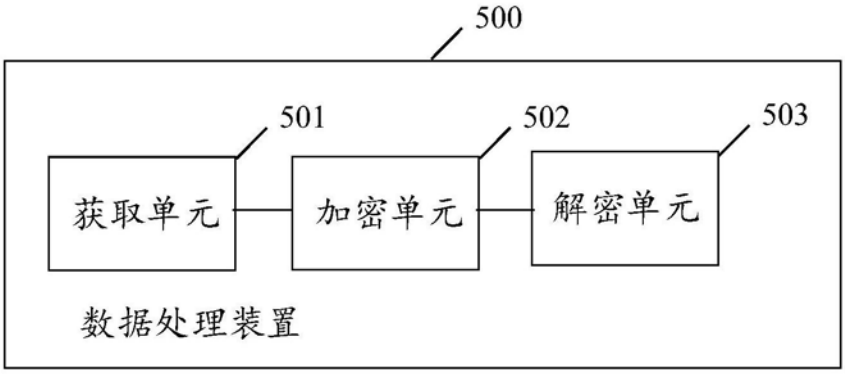

500
501
502
503
获取单元
加密单元
解密单元
数据处理装置

图5

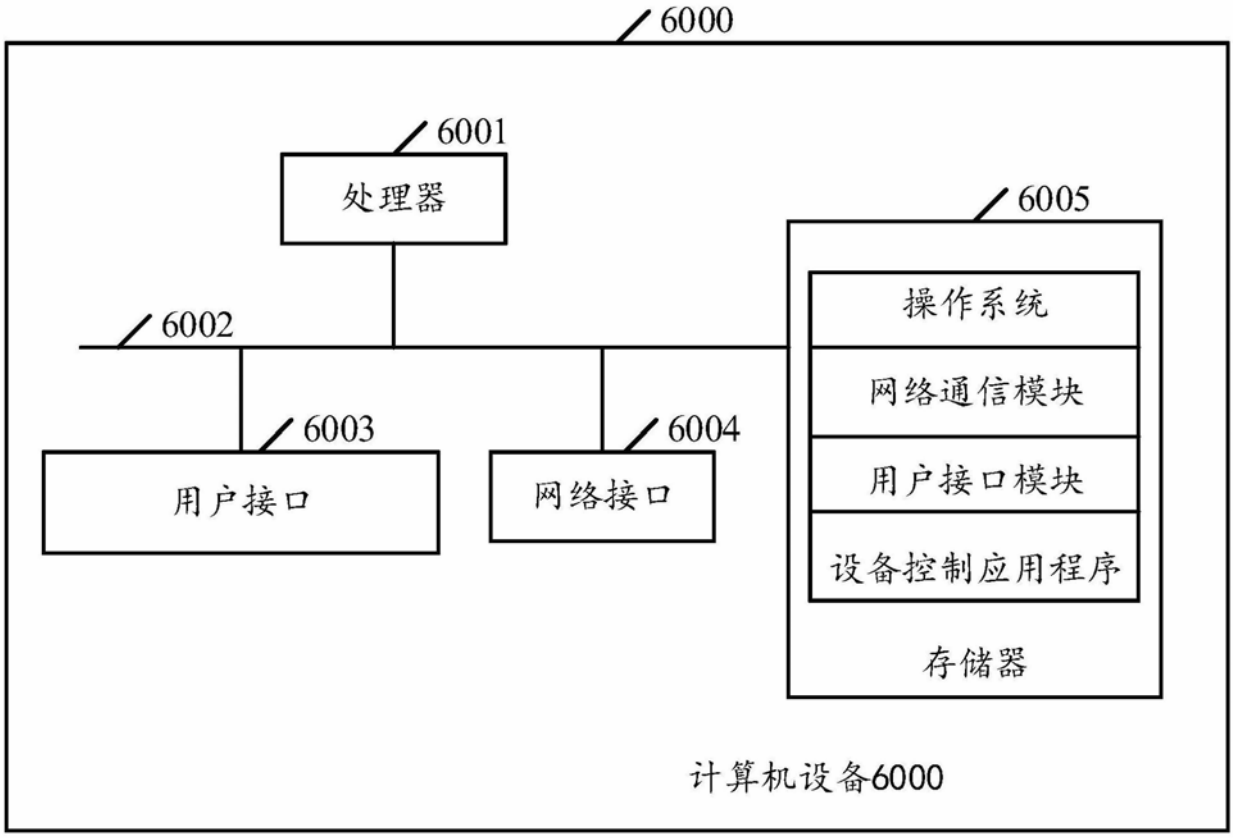

6000
6001
处理器
6005
操作系统
网络通信模块
用户接口模块
设备控制应用程序
存储器
6002
6003
用户接口
6004
网络接口
计算机设备6000

图6

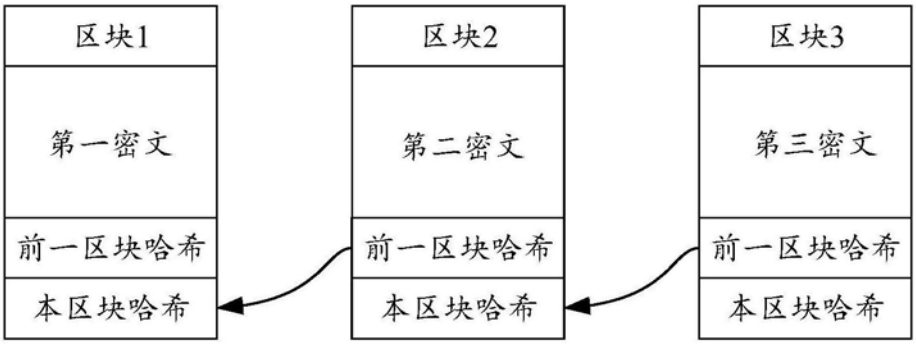

区块1
第一密文
前一区块哈希
本区块哈希
区块2
第二密文
前一区块哈希
本区块哈希
区块3
第三密文
前一区块哈希
本区块哈希

图7