(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 110839026 A
(43)申请公布日 2020.02.25

(21)申请号 201911101715.5

(22)申请日 2019.11.12

(71)申请人 深圳市网心科技有限公司
地址 518063 广东省深圳市南山区高新南九道9号威新软件园5号楼5层

(72)发明人 张骁

(74)专利代理机构 深圳市赛恩倍吉知识产权代理有限公司 44334
代理人 何春兰

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)
H04L 9/06(2006.01)
H04L 9/08(2006.01)
H04L 9/30(2006.01)

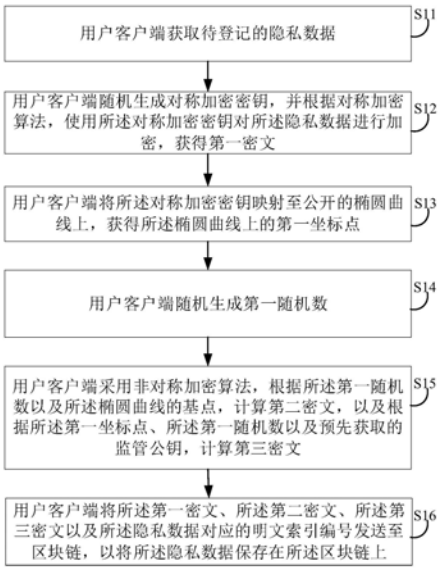
权利要求书3页 说明书15页 附图5页

(54)发明名称

基于区块链的数据处理方法及相关设备

(57)摘要

一种基于区块链的数据处理方法，包括：获取待登记的隐私数据；随机生成对称加密密钥，并根据对称加密算法，使用所述对称加密密钥对所述隐私数据进行加密，获得第一密文；将对称加密密钥映射至公开的椭圆曲线上，获得椭圆曲线上的第一坐标点；随机生成第一随机数；采用非对称加密算法，根据第一随机数以及椭圆曲线的基点，计算第二密文，以及根据第一坐标点、第一随机数以及预先获取的监管公钥，计算第三密文；将第一密文、第二密文、第三密文以及隐私数据对应的明文索引编号发送至区块链，以将所述隐私数据保存在所述区块链上。本发明还提供一种用户客户端、监管客户端及存储介质。本发明能够对数据进行有效记录，同时，确保数据的安全。



CN 110839026 A

1.一种基于区块链的数据处理方法,应用于用户客户端,其特征在于,所述方法包括:

获取待登记的隐私数据;

随机生成对称加密密钥,并根据对称加密算法,使用所述对称加密密钥对所述隐私数据进行加密,获得第一密文;

将所述对称加密密钥映射至公开的椭圆曲线上,获得所述椭圆曲线上的第一坐标点;

随机生成第一随机数;

采用非对称加密算法,根据所述第一随机数以及所述椭圆曲线的基点,计算第二密文,以及根据所述第一坐标点、所述第一随机数以及预先获取的监管公钥,计算第三密文;

将所述第一密文、所述第二密文、所述第三密文以及所述隐私数据对应的明文索引编号发送至区块链,以将所述隐私数据保存在所述区块链上。

2.根据权利要求1所述的方法,其特征在于,在所述获取待登记的隐私数据之前,所述方法还包括:

获取由监管方公开的椭圆曲线公共参数以及监管公钥,其中,所述椭圆曲线公共参数包括椭圆曲线的基点G和椭圆曲线的线阶n;

所述随机生成第一随机数包括:随机生成小于n的第一随机数k;

所述采用非对称加密算法,根据所述第一随机数以及所述椭圆曲线的基点,计算第二密文,以及根据所述第一坐标点、所述第一随机数以及预先获取的监管公钥,计算第三密文包括:

利用如下公式计算第二密文和第三密文:$\begin{cases} C_1 = k \cdot G \\ C_2 = M + k \cdot Y \end{cases}$;其中,M表示所述第一坐标点,Y表示所述监管公钥,C1表示所述第二密文,C2表示所述第三密文。

3.根据权利要求1所述的方法,其特征在于,所述方法还包括:

将所述第一随机数映射成密钥二维码;

将所述密钥二维码与所述明文索引编号输出在隐私数据登记簿上。

4.根据权利要求3所述的方法,其特征在于,所述方法还包括:

获取待查询的目标明文索引编号和目标密钥二维码;

向所述区块链发送所述目标明文索引编号,以获取所述区块链上保存的目标密文,所述目标密文包括目标第一密文、目标第二密文和目标第三密文;

读取所述目标密钥二维码,获得目标随机数;

根据所述目标第三密文、所述目标随机数以及所述监管公钥,计算目标对称加密密钥映射在所述椭圆曲线上的目标坐标点;

根据所述椭圆曲线上坐标点的映射规则,确定所述目标坐标点对应的目标对称加密密钥;

利用所述目标对称加密密钥,对所述目标第一密文进行解密,获得目标隐私数据。

5.根据权利要求1至4中任一项所述的方法,其特征在于,所述将所述第一密文、所述第二密文、所述第三密文以及所述隐私数据对应的明文索引编号发送至区块链上之前,所述方法还包括:

获取所述隐私数据所属用户的用户标识;

采用哈希算法,根据所述用户标识,生成所述隐私数据对应的明文索引编号。

6.一种基于区块链的数据处理方法，应用于监管客户端，其特征在于，所述方法包括：

从区块链上获取待监管密文，所述待监管密文包括第一密文、第二密文和第三密文；

获取预先保存的监管私钥；

根据所述监管私钥、所述第二密文和所述第三密文，计算第一对称加密密钥映射在椭圆曲线上的第一坐标点；

根据所述椭圆曲线上坐标点的映射规则，确定所述第一坐标点对应的第一对称加密密钥；

利用所述第一对称加密密钥，对所述第一密文进行解密，获得监管数据。

7.根据权利要求6所述的方法，其特征在于，所述根据所述监管私钥以及所述第二密文和所述第三密文，计算第一对称加密密钥映射在椭圆曲线上的第一坐标点包括：

利用如下公式计算目标坐标点：$C_2-x\cdot C_1=M$；

其中，C1表示所述第二密文，C2表示所述第三密文，x表示所述监管私钥，M表示所述第一坐标点。

8.根据权利要求7所述的方法，其特征在于，所述从区块链上获取待监管密文之前，所述方法还包括：

获取由监管方公开的椭圆曲线公共参数，其中，所述椭圆曲线公共参数包括椭圆曲线的线阶n；

随机生成小于n的随机数x，并将所述随机数x确定为监管私钥；

保存所述监管私钥。

9.根据权利要求6所述的方法，其特征在于，所述方法还包括：

获取用户标识；

对所述用户标识进行身份验证；

若所述身份验证成功，采用哈希算法，根据所述用户标识，生成待挂失数据对应的明文索引编号；

从所述区块链上，获取所述明文索引编号对应的历史密文，所述历史密文包括历史第一密文、历史第二密文和历史第三密文；

根据所述监管私钥、所述历史第二密文和所述历史第三密文，计算第二对称加密密钥映射在所述椭圆曲线上的第二坐标点；

根据所述椭圆曲线上坐标点的映射规则，确定所述第二坐标点对应的第二对称加密密钥；

利用所述第二对称加密密钥，对所述历史第一密文进行解密，获得所述待挂失数据；

根据所述待挂失数据，生成隐私数据登记簿。

10.一种用户客户端，其特征在于，所述用户客户端包括处理器和存储器，所述处理器用于执行存储器中存储的计算机程序以实现如权利要求1至5中任意一项所述的基于区块链的数据处理方法。

11.一种监管客户端，其特征在于，所述监管客户端包括处理器和存储器，所述处理器用于执行存储器中存储的计算机程序以实现如权利要求6至9中任意一项所述的基于区块链的数据处理方法。

12.一种计算机可读存储介质，其特征在于，所述计算机可读存储介质存储有至少一个

指令,所述至少一个指令被处理器执行时实现如权利要求1至5或6至9中任意一项所述的基于区块链的数据处理方法。

基于区块链的数据处理方法及相关设备

技术领域

[0001] 本发明涉及区块链技术领域，尤其涉及一种基于区块链的数据处理方法及相关设备。

背景技术

[0002] 随着大数据的兴起，各行各业对数据的收集、处理、交易和应用越来越频繁。然而，现阶段，对数据的记录仍然依赖于局部中心化信息系统或第三方平台，这种记录方案不够健全，同时，用户的隐私数据(比如疫苗隐私数据)很容易被篡改或泄露，使得数据的安全受到威胁。

[0003] 因此，如何对数据进行有效记录，以确保数据的安全是一个亟待解决的技术问题。

发明内容

[0004] 鉴于以上内容，有必要提供一种基于区块链的数据处理方法及相关设备，能够对数据进行有效记录，同时，确保数据的安全。

[0005] 本发明的第一方面提供一种基于区块链的数据处理方法，应用于用户客户端，所述方法包括：

[0006] 获取待登记的隐私数据；

[0007] 随机生成对称加密密钥，并根据对称加密算法，使用所述对称加密密钥对所述隐私数据进行加密，获得第一密文；

[0008] 将所述对称加密密钥映射至公开的椭圆曲线上，获得所述椭圆曲线上的第一坐标点；

[0009] 随机生成第一随机数；

[0010] 采用非对称加密算法，根据所述第一随机数以及所述椭圆曲线的基点，计算第二密文，以及根据所述第一坐标点、所述第一随机数以及预先获取的监管公钥，计算第三密文；

[0011] 将所述第一密文、所述第二密文、所述第三密文以及所述隐私数据对应的明文索引编号发送至区块链，以将所述隐私数据保存在所述区块链上。

[0012] 在一种可能的实现方式中，所述方法还包括：

[0013] 在所述获取待登记的隐私数据之前，所述方法还包括：

[0014] 获取由监管方公开的椭圆曲线公共参数以及监管公钥，其中，所述椭圆曲线公共参数包括椭圆曲线的基点G和椭圆曲线的线阶n；

[0015] 所述随机生成第一随机数包括：随机生成小于n的第一随机数k；

[0016] 所述采用非对称加密算法，根据所述第一随机数以及所述椭圆曲线的基点，计算第二密文，以及根据所述第一坐标点、所述第一随机数以及预先获取的监管公钥，计算第三密文包括：

[0017] 利用如下公式计算第二密文和第三密文：$\begin{cases} C_1 = k \cdot G \\ C_2 = M + k \cdot Y \end{cases}$；其中，M表示所述第一坐标点，Y表示所述监管公钥，C1表示所述第二密文，C2表示所述第三密文。

[0018] 在一种可能的实现方式中，所述方法还包括：

[0019] 将所述第一随机数映射成密钥二维码；

[0020] 将所述密钥二维码与所述明文索引编号输出在隐私数据登记簿上

[0021] 在一种可能的实现方式中，所述方法还包括：

[0022] 获取待查询的目标明文索引编号和目标密钥二维码；

[0023] 向所述区块链发送所述目标明文索引编号，以获取所述区块链上保存的目标密文，所述目标密文包括目标第一密文、目标第二密文和目标第三密文；

[0024] 读取所述目标密钥二维码，获得目标随机数；

[0025] 根据所述目标第三密文、所述目标随机数以及所述监管公钥，计算目标对称加密密钥映射在所述椭圆曲线上的目标坐标点；

[0026] 根据所述椭圆曲线上坐标点的映射规则，确定所述目标坐标点对应的目标对称加密密钥；

[0027] 利用所述目标对称加密密钥，对所述目标第一密文进行解密，获得目标隐私数据。

[0028] 在一种可能的实现方式中，所述将所述第一密文、所述第二密文、所述第三密文以及所述隐私数据对应的明文索引编号发送至区块链，以将所述隐私数据保存在所述区块链上之前，所述方法还包括：

[0029] 获取所述隐私数据所属用户的用户标识；

[0030] 采用哈希算法，根据所述用户标识，生成所述隐私数据对应的明文索引编号。

[0031] 本发明的第二方面提供一种基于区块链的数据处理方法，应用于监管客户端，所述方法包括：

[0032] 从区块链上获取待监管密文，所述待监管密文包括第一密文、第二密文和第三密文；

[0033] 获取预先保存的监管私钥；

[0034] 根据所述监管私钥、所述第二密文和所述第三密文，计算第一对称加密密钥映射在椭圆曲线上的第一坐标点；

[0035] 根据所述椭圆曲线上坐标点的映射规则，确定所述第一坐标点对应的第一对称加密密钥；

[0036] 利用所述第一对称加密密钥，对所述第一密文进行解密，获得监管数据。

[0037] 在一种可能的实现方式中，所述方法还包括：

[0038] 所述根据所述监管私钥以及所述第二密文和所述第三密文，计算第一对称加密密钥映射在椭圆曲线上的第一坐标点包括：

[0039] 利用如下公式计算目标坐标点：$C_2-x \cdot C_1=M$；

[0040] 其中，C1表示所述第二密文，C2表示所述第三密文，x表示所述监管私钥，M表示所述第一坐标点。

[0041] 在一种可能的实现方式中，所述从区块链上获取待监管密文之前，所述方法还包括：

[0042] 获取由监管方公开的椭圆曲线公共参数，其中，所述椭圆曲线公共参数包括椭圆曲线的线阶n；

[0043] 随机生成小于n的随机数x，并将所述随机数x确定为监管私钥；

[0044] 保存所述监管私钥。

[0045] 在一种可能的实现方式中，所述方法还包括：

[0046] 获取用户标识；

[0047] 对所述用户标识进行身份验证；

[0048] 若所述身份验证成功，采用哈希算法，根据所述用户标识，生成待挂失数据对应的明文索引编号；

[0049] 从所述区块链上，获取所述明文索引编号对应的历史密文，所述历史密文包括历史第一密文、历史第二密文和历史第三密文；

[0050] 根据所述监管私钥、所述历史第二密文和所述历史第三密文，计算第二对称加密密钥映射在所述椭圆曲线上的第二坐标点；

[0051] 根据所述椭圆曲线上坐标点的映射规则，确定所述第二坐标点对应的第二对称加密密钥；

[0052] 利用所述第二对称加密密钥，对所述历史第一密文进行解密，获得所述待挂失数据；

[0053] 根据所述待挂失数据，生成隐私数据登记簿。

[0054] 本发明的第三方面提供一种用户客户端，所述用户客户端包括处理器和存储器，所述处理器用于执行存储器中存储的计算机程序以实现第一方面所述的基于区块链的数据处理方法。

[0055] 本发明的第四方面提供一种监管客户端，所述监管客户端包括处理器和存储器，所述处理器用于执行存储器中存储的计算机程序以实现第二方面所述的基于区块链的数据处理方法。

[0056] 本发明的第五方面提供一种计算机可读存储介质，所述计算机可读存储介质上存储有计算机程序，所述计算机程序被处理器执行时实现所述的基于区块链的数据处理方法。

[0057] 由以上技术方案，本发明中，通过对称加密密钥以及非对称加密算法对用户的隐私数据进行隐私保护处理，获得了第一密文、第二密文以及第三密文，保证了隐私数据能够以密文形式传送至区块链，同时，利用区块链上的数据具有不可篡改的性质，将密文数据发送至区块链存储，可以有效对隐私数据进行追踪记录，从而能够提供健全有效的数据记录，同时，确保数据的安全。

附图说明

[0058] 图1是本发明公开的一种基于区块链的数据处理方法的较佳实施例的流程图。

[0059] 图2是本发明公开的一种疫苗接种本的示意图。

[0060] 图3是本发明公开的另一种基于区块链的数据处理方法的较佳实施例的流程图。

[0061] 图4是本发明公开的一种数据处理装置的较佳实施例的功能模块图。

[0062] 图5是本发明公开的另一种数据处理装置的较佳实施例的功能模块图。

[0063] 图6是本发明实现基于区块链的数据处理方法的较佳实施例的用户客户端的结构示意图。

[0064] 图7是本发明实现基于区块链的数据处理方法的较佳实施例的监管客户端的结构示意图。

具体实施方式

[0065] 为了使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅用以解释本发明，并不用于限定本发明。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0066] 本申请的说明书和权利要求书及上述附图中的术语“第一”、“第二”、“第三”是用于区别类似的对象，而不必用于描述特定的顺序或先后次序，也不能理解为指示或暗示其相对重要性或者隐含指明所指示的技术特征的数量。应该理解这样使用的数据在适当情况下可以互换，以便这里描述的实施例能够以除了在这里图示或描述的内容以外的顺序实施，限定有“第一”、“第二”、“第三”的特征可以明示或者隐含地包括至少一个该特征。

[0067] 此外，术语“包括”和“具有”以及他们的任何变形，意图在于覆盖不排他的包含，例如，包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。

[0068] 另外，各个实施例之间的技术方案可以相互结合，但是必须是以本领域普通技术人员能够实现为基础，当技术方案的结合出现相互矛盾或无法实现时应当认为这种技术方案的结合不存在，也不在本发明要求的保护范围之内。

[0069] 用户客户端或监管客户端均是一种能够按照事先设定或存储的指令，自动进行数值计算和/或信息处理的设备，其硬件包括但不限于微处理器、专用集成电路(ASIC)、现场可编程门阵列(FPGA)、数字处理器(DSP)、嵌入式设备等。所述用户客户端或监管客户端可以是网络服务器，也可以是任何一种可与用户通过键盘、鼠标、遥控器、触摸板或声控设备等方式进行人机交互的电子产品，例如，个人计算机、平板电脑、智能手机、个人数字助理PDA等。

[0070] 请参见图1，图1是本发明公开的一种基于区块链的数据处理方法的较佳实施例的流程图。其中，该数据处理方法应用于用户客户端中，根据不同的需求，该流程图中步骤的顺序可以改变，某些步骤可以省略。

[0071] S11、用户客户端获取待登记的隐私数据。

[0072] 其中，隐私数据可以包括但不限于疫苗接种数据、病历数据、交通违章数据、房产交易数据、学术考试成绩数据、学历学位数据等。

[0073] S12、用户客户端随机生成对称加密密钥，并根据对称加密算法，使用所述对称加密密钥对所述隐私数据进行加密，获得第一密文。

[0074] 其中，所述对称加密算法可以包括但不限于AES或SM4算法。

[0075] 本发明中，可以采用随机数生成器随机生成对称加密密钥，然后，根据AES或SM4算法，使用所述对称加密密钥对所述隐私数据进行加密，获得第一密文。通过所述第一密文，

实现了对所述隐私数据的加密，保护了用户的隐私数据。

[0076] S13、用户客户端将所述对称加密密钥映射至公开的椭圆曲线上，获得所述椭圆曲线上的第一坐标点。

[0077] 可选的，在步骤S11之前，所述方法还可以包括：

[0078] 获取由监管方公开的椭圆曲线公共参数以及监管公钥，其中，所述椭圆曲线公共参数包括椭圆曲线的基点G和椭圆曲线的线阶n；

[0079] 本发明中，可以利用椭圆曲线映射规则将所述对称加密密钥映射至公开的椭圆曲线上，获得所述椭圆曲线上的第一坐标点。

[0080] 其中，预先可以选取长度为256bit的椭圆曲线，并公开相关公共参数，比如椭圆曲线基点G和椭圆曲线的阶n。

[0081] 其中，椭圆曲线映射规则如下：

[0082] 例如待映射数据为m，椭圆曲线方程为y＝f(x)，则可以使x＝m，代入椭圆曲线方程求得y＝f(m)，最后得到的椭圆曲线的坐标点(x,y)，即为m映射到椭圆曲线的坐标点。

[0083] S14、用户客户端随机生成第一随机数。

[0084] 其中，用户客户端可以利用随机数生成器或是相关算法随机生成第一随机数，其中，所述第一随机数的取值k需要小于椭圆曲线的线阶n。

[0085] 其中，可以将所述第一随机数确定作为加密所述对称加密密钥的秘钥，以对所述对称加密密钥进行保护。

[0086] S15、用户客户端采用非对称加密算法，根据所述第一随机数以及所述椭圆曲线的基点，计算第二密文，以及根据所述第一坐标点、所述第一随机数以及预先获取的监管公钥，计算第三密文。

[0087] 其中，非对称加密算法可以包括但不限于非对称EL Gamal加密算法。通常，非对称EL Gamal加密算法是基于离散对数问题(discrete logarithm problem,DLP)问题的，本发明中把El Gamal的安全性问题转移到了椭圆曲线离散对数问题(elliptic curve discrete logarithm problem,ECDLP)上。

[0088] 具体的，用户客户端采用非对称加密算法，根据所述第一随机数以及所述椭圆曲线的基点，计算第二密文，以及根据所述第一坐标点、所述第一随机数以及预先获取的监管公钥，计算第三密文包括：

[0089] 利用如下公式计算第二密文和第三密文：$\begin{cases} C_1 = k \cdot G \\ C_2 = M + k \cdot Y \end{cases}$；

[0090] 其中，M表示所述第一坐标点，Y表示所述监管公钥，C1表示所述第二密文，C2表示所述第三密文，k为所述第一随机数。

[0091] S16、用户客户端将所述第一密文、所述第二密文、所述第三密文以及所述隐私数据对应的明文索引编号发送至区块链，以将所述隐私数据保存在所述区块链上。

[0092] 优选的，在步骤S16中，用户客户端可以预先在区块链系统注册账号，并获取公私钥，利用私钥对所述第一密文、所述第二密文、所述第三密文以及明文索引编号进行签名后，将所述第一密文、所述第二密文、所述第三密文、明文索引编号与签名一起发送至区块链，区块链系统利用该用户客户端的公玥验签所述签名后，将所述第一密文、所述第二密文、所述第三密文、明文索引编号保存在区块链上。

[0093] 作为一种可选的实施方式，步骤S16用户客户端将所述第一密文、所述第二密文、所述第三密文以及所述隐私数据对应的明文索引编号发送至区块链，以将所述隐私数据保存在所述区块链上之前，所述方法还包括：

[0094] 获取所述隐私数据所属用户的用户标识；

[0095] 采用哈希算法，根据所述用户标识，生成所述隐私数据对应的明文索引编号。

[0096] 其中，所述用户标识比如用户姓名、用户身份证号码等，该用户标识可以唯一标识用户的身份。

[0097] 可选的，可以采用如下编码方式计算明文索引编号：

[0098] 采用哈希算法，根据用户姓名、用户身份证号码，获得哈希值，在对哈希值进行Base58转码，获得所述隐私数据对应的明文索引编号。

[0099] 作为一种可选的实施方式，所述方法还包括：

[0100] 将所述第一随机数映射成密钥二维码；

[0101] 将所述密钥二维码与所述明文索引编号输出在隐私数据登记簿上。

[0102] 在该实施方式中，可以根据二维码映射规则，将所述第一随机数映射成密钥二维码，其中，二维码映射是根据通用的二维码生成标准进行映射的，比如国家标准GB/T 18284-2000。

[0103] 其中，隐私数据登记簿可以是电子的，例如可以是终端设备(例如手机或电脑)上的一个软件，则将所述密钥二维码与所述明文索引编号输出在隐私数据登记簿上可以是通过网络将所述密钥二维码与所述明文索引编号下发至该终端设备；当然也可以是实体的，例如纸质的，如果是实体的，则可以通过打印设备将所述密钥二维码与所述明文索引编号打印在登记簿上。

[0104] 所述隐私数据登记簿比如疫苗接种本，图2是本发明公开的一种疫苗接种本的示意图。

[0105] 如图2所示，疫苗接种本上可以包括接种用户的身份信息以及接种记录，身份信息比如姓名张三，身份证号：XXXXXXXXX，接种记录比如疫苗类型、接种日期、地点编号以及疫苗批次，此外，还包括链上编号(即明文索引编号)以及密钥二维码。不同的接种记录对应不同的链上编号以及不同的密钥二维码。

[0106] 作为一种可选的实施方式，所述方法还包括：

[0107] 获取待查询的目标明文索引编号和目标密钥二维码；

[0108] 向所述区块链发送所述目标明文索引编号，以获取所述区块链上保存的目标密文，所述目标密文包括目标第一密文、目标第二密文和目标第三密文；

[0109] 读取所述目标密钥二维码，获得目标随机数；

[0110] 根据所述目标第三密文、所述目标随机数以及所述监管公钥，计算目标对称加密密钥映射在所述椭圆曲线上的目标坐标点；

[0111] 根据所述椭圆曲线上坐标点的映射规则，确定所述目标坐标点对应的目标对称加密密钥；

[0112] 利用所述目标对称加密密钥，对所述目标第一密文进行解密，获得目标隐私数据。

[0113] 在该实施方式中，当需要查询数据记录时，可以获取隐私数据处理簿上的明文索引编号和密钥二维码，并向所述区块链发送所述目标明文索引编号，以获取所述区块链上

保存的目标密文(目标第一密文、目标第二密文和目标第三密文),同时,还可以读取所述目标密钥二维码,获得所述目标随机数,其中,目标第一密文、目标第二密文和目标第三密文与上文所述的第一密文、第二密文和第三密文的计算方式相同,目标随机数与上文所述的第一随机数的计算方式相同,可以参照上述第三密文的计算公式$C_2=M+k\cdot Y$,获得公式$M=C_2-k\cdot Y$,然后,令C_2为目标第三密文,k为目标随机数,Y为监管公钥,M为目标坐标点,代入公式$M=C_2-k\cdot Y$,即可计算目标对称加密密钥映射在所述椭圆曲线上的目标坐标点,并根据所述椭圆曲线上坐标点的映射规则,确定所述目标坐标点对应的目标对称加密密钥,最后,即可利用所述目标对称加密密钥,对所述目标第一密文进行解密,获得目标隐私数据。

[0114] 其中,解密算法与上述对称加密算法是相反的过程。

[0115] 在图1所描述的方法流程中,可以通过对称加密密钥以及非对称加密算法对用户的隐私数据进行隐私保护处理,获得了第一密文、第二密文以及第三密文,保证了隐私数据能够以密文形式传送至区块链,同时,利用区块链上的数据具有不可篡改的性质,将密文数据发送至区块链存储,可以有效对隐私数据进行追踪记录,从而能够提供健全有效的数据记录,同时,确保数据的安全。

[0116] 请参见图3,图3是本发明公开的另一种基于区块链的数据处理方法的较佳实施例的流程图。其中,该数据处理方法应用于监管客户端中,根据不同的需求,该流程图中步骤的顺序可以改变,某些步骤可以省略。

[0117] S31、监管客户端从区块链上获取待监管密文,所述待监管密文包括第一密文、第二密文和第三密文。

[0118] 其中,监管客户端可以从区块链上获取任意需要监管的待监管密文。

[0119] S32、监管客户端获取预先保存的监管私钥。

[0120] 作为一种可选的实施方式,步骤S31所述从区块链上获取待监管密文之前,所述方法还包括:

[0121] 获取由监管方公开的椭圆曲线公共参数,其中,所述椭圆曲线公共参数包括椭圆曲线的线阶n;

[0122] 随机生成小于n的随机数x,并将所述随机数x确定为监管私钥;

[0123] 保存所述监管私钥。

[0124] 在该实施方式中,可以获取由监管方公开的椭圆曲线公共参数,比如椭圆曲线基点G和椭圆曲线的线阶n。其中,椭圆曲线可以选取长度为256bit的椭圆曲线。

[0125] 可以采用随机数生成器或是相关算法随机生成小于n的随机数x,并将所述随机数x确定为监管私钥,所述监管私钥可以由监管方(比如省疾控中心)保存。

[0126] 此外,可以根据公式$Y=x\cdot G$来计算监管公钥,其中,Y为监管公钥,x为监管私钥,G为椭圆曲线的基点。在计算获得监管公钥之后,即可将公钥对外公开。

[0127] S33、监管客户端根据所述监管私钥、所述第二密文和所述第三密文,计算第一对称加密密钥映射在椭圆曲线上的第一坐标点。

[0128] 其中,椭圆曲线映射规则如下:

[0129] 例如待映射数据为m,椭圆曲线方程为$y=f(x)$,则可以使$x=m$,代入椭圆曲线方程求得$y=f(m)$,最后得到的椭圆曲线的坐标点(x,y),即为m映射到椭圆曲线的坐标点。

[0130] 具体的,所述根据所述监管私钥以及所述第二密文和所述第三密文,计算第一对

称加密密钥映射在椭圆曲线上的第一坐标点包括：

[0131] 利用如下公式计算目标坐标点：$C_2-x\cdot C_1=M$；

[0132] 其中，C1表示所述第二密文，C2表示所述第三密文，x表示所述监管私钥，M表示所述第一坐标点。

[0133] 其中，上述公式$C_2-x\cdot C_1=M$的推导过程如下：

[0134] $C_2-x\cdot C_1=M+k\cdot Y-xk\cdot G=M+xk\cdot G-xk\cdot G=M$

[0135] 其中，该推导过程可以参考图1中关于第二密文和第三密文的计算方式：$\begin{cases} C_1=k\cdot G \\ C_2=M+k\cdot Y \end{cases}$，具体可以参考图1中的相关描述，在此不再赘述。

[0136] S34、监管客户端根据所述椭圆曲线上坐标点的映射规则，确定所述第一坐标点对应的第一对称加密密钥。

[0137] S35、监管客户端利用所述第一对称加密密钥，对所述第一密文进行解密，获得监管数据。

[0138] 其中，监管方持有监管密钥，可以解开任何加密信息，而其他用户在不拥有数据加密密钥的情况下，无法解开加密信息。

[0139] 作为一种可选的实施方式，所述方法还包括：

[0140] 获取用户标识；

[0141] 对所述用户标识进行身份验证；

[0142] 若所述身份验证成功，采用哈希算法，根据所述用户标识，生成待挂失数据对应的明文索引编号；

[0143] 从所述区块链上，获取所述明文索引编号对应的历史密文，所述历史密文包括历史第一密文、历史第二密文和历史第三密文；

[0144] 根据所述监管私钥、所述历史第二密文和所述历史第三密文，计算第二对称加密密钥映射在所述椭圆曲线上的第二坐标点；

[0145] 根据所述椭圆曲线上坐标点的映射规则，确定所述第二坐标点对应的第二对称加密密钥；

[0146] 利用所述第二对称加密密钥，对所述历史第一密文进行解密，获得所述待挂失数据；

[0147] 根据所述待挂失数据，生成隐私数据登记簿。

[0148] 在该实施方式中，当用户的隐私数据丢失后，可以通过监管方查询。具体的，用户可以向监管方提供用户的身份标识(比如用户姓名、身份证号码)，监管客户端获取到用户标识后，可以对所述用户标识进行身份验证，在验证成功后，即可帮接种用户找回丢失的隐私数据。具体的，可以根据上文所述的编码方式，通过用户姓名以及用户身份证号码计算得到明文索引编号，进而从所述区块链上，获取所述明文索引编号对应的历史密文，并根据上文所述的解密方法对所述历史密文进行解密，获得待挂失数据(即丢失的隐私数据)，最后即可根据所述待挂失数据，重新生成隐私数据登记簿。其中，可以以疫苗接种数据为例，隐私数据登记簿参考图2中所述的疫苗接种本。

[0149] 在图3所描述的方法流程中，监管客户端可以从区块链上拉取任意的密文数据，并使用监管私钥，对密文数据进行解密，获得用户的隐私数据，并对隐私数据实现监管，而其

他用户，在不拥有监管私钥的前提下，是无法解开区块链上的密文数据的，从而可以保护用户的隐私数据。

[0150] 以上所述，仅是本发明的具体实施方式，但本发明的保护范围并不局限于此，对于本领域的普通技术人员来说，在不脱离本发明创造构思的前提下，还可以做出改进，但这些均属于本发明的保护范围。

[0151] 请参见图4，图4是本发明公开的一种数据处理装置的较佳实施例的功能模块图。

[0152] 在一些实施例中，所述数据处理装置运行于用户客户端中。所述数据处理装置可以包括多个由程序代码段所组成的功能模块。所述数据处理装置中的各个程序段的程序代码可以存储于存储器中，并由至少一个处理器所执行，以执行图1所描述的基于区块链的数据处理方法中的部分或全部步骤，具体请参照图1中的相关描述，在此不再赘述。

[0153] 本实施例中，所述数据处理装置根据其所执行的功能，可以被划分为多个功能模块。所述功能模块可以包括：获取模块401、生成模块402、加密模块403、映射模块404、计算模块405及发送模块406。本发明所称的模块是指一种能够被至少一个处理器所执行并且能够完成固定功能的一系列计算机程序段，其存储在存储器中。

[0154] 获取模块401，用于获取待登记的隐私数据；

[0155] 生成模块402，用于随机生成对称加密密钥；

[0156] 加密模块403，用于使用所述对称加密密钥对所述隐私数据进行加密，获得第一密文；

[0157] 映射模块404，用于将所述对称加密密钥映射至公开的椭圆曲线上，获得所述椭圆曲线上的第一坐标点；

[0158] 所述生成模块402，还用于随机生成第一随机数；

[0159] 计算模块405，用于采用非对称加密算法，根据所述第一随机数以及所述椭圆曲线的基点，计算第二密文，以及根据所述第一坐标点、所述第一随机数以及预先获取的监管公钥，计算第三密文；

[0160] 发送模块406，用于将所述第一密文、所述第二密文、所述第三密文以及所述隐私数据对应的明文索引编号发送至区块链，以将所述隐私数据保存在所述区块链上。

[0161] 可选的，所述获取模块401，还用于获取由监管方公开的椭圆曲线公共参数以及监管公钥，其中，所述椭圆曲线公共参数包括椭圆曲线的基点G和椭圆曲线的线阶n；

[0162] 所述生成模块402随机生成第一随机数包括：随机生成小于n的第一随机数k；

[0163] 所述计算模块405采用非对称加密算法，根据所述第一随机数以及所述椭圆曲线的基点，计算第二密文，以及根据所述第一坐标点、所述第一随机数以及预先获取的监管公钥，计算第三密文包括：

[0164] 利用如下公式计算第二密文和第三密文：$\begin{cases} C_1 = k \cdot G \\ C_2 = M + k \cdot Y \end{cases}$；其中，M表示所述第一坐标点，Y表示所述监管公钥，C1表示所述第二密文，C2表示所述第三密文。

[0165] 可选的，所述映射模块404，还用于将所述第一随机数映射成密钥二维码；

[0166] 所述数据处理装置还包括：

[0167] 输出模块，用于将所述密钥二维码与所述明文索引编号输出在隐私登记处理簿上。

[0168] 可选的，所述获取模块401，还用于获取待查询的目标明文索引编号和目标密钥二维码；

[0169] 所述发送模块406，还用于向所述区块链发送所述目标明文索引编号，以获取所述区块链上保存的目标密文，所述目标密文包括目标第一密文、目标第二密文和目标第三密文；

[0170] 所述数据处理装置还包括：

[0171] 读取模块，用于读取所述目标密钥二维码，获得目标随机数；

[0172] 所述计算模块405，还用于根据所述目标第三密文、所述目标随机数以及所述监管公钥，计算目标对称加密密钥映射在所述椭圆曲线上的目标坐标点；

[0173] 确定模块，用于根据所述椭圆曲线上坐标点的映射规则，确定所述目标坐标点对应的目标对称加密密钥；

[0174] 解密模块，用于利用所述目标对称加密密钥，对所述目标第一密文进行解密，获得目标隐私数据。

[0175] 可选的，所述获取模块401，还用于获取所述隐私数据所属用户的用户标识；

[0176] 所述生成模块402，还用于采用哈希算法，根据所述用户标识，生成所述隐私数据对应的明文索引编号。

[0177] 在图4所描述的数据处理装置中，可以通过对称加密密钥以及非对称加密算法对用户的隐私数据进行隐私保护处理，获得了第一密文、第二密文以及第三密文，保证了隐私数据能够以密文形式传送至区块链，同时，利用区块链上的数据具有不可篡改的性质，将密文数据发送至区块链存储，可以有效对隐私数据进行追踪记录，从而能够提供健全有效的数据记录，同时，确保数据的安全。

[0178] 请参见图5，图5是本发明公开的另一种数据处理装置的较佳实施例的功能模块图。

[0179] 在一些实施例中，所述数据处理装置运行于监管客户端中。所述数据处理装置可以包括多个由程序代码段所组成的功能模块。所述数据处理装置中的各个程序段的程序代码可以存储于存储器中，并由至少一个处理器所执行，以执行图3所描述的基于区块链的数据处理方法中的部分或全部步骤，具体请参照图3中的相关描述，在此不再赘述。

[0180] 本实施例中，所述数据处理装置根据其所执行的功能，可以被划分为多个功能模块。所述功能模块可以包括：获取模块501、计算模块502、确定模块503及解密模块504。本发明所称的模块是指一种能够被至少一个处理器所执行并且能够完成固定功能的一系列计算机程序段，其存储在存储器中。

[0181] 获取模块501，用于从区块链上获取待监管密文，所述待监管密文包括第一密文、第二密文和第三密文；

[0182] 所述获取模块501，还用于获取预先保存的监管私钥；

[0183] 计算模块502，用于根据所述监管私钥、所述第二密文和所述第三密文，计算第一对称加密密钥映射在椭圆曲线上的第一坐标点；

[0184] 确定模块503，用于根据所述椭圆曲线上坐标点的映射规则，确定所述第一坐标点对应的第一对称加密密钥；

[0185] 解密模块504，用于利用所述第一对称加密密钥，对所述第一密文进行解密，获得

监管数据。

[0186] 可选的，所述计算模块502根据所述监管私钥以及所述第二密文和所述第三密文，计算第一对称加密密钥映射在椭圆曲线上的第一坐标点包括：

[0187] 利用如下公式计算目标坐标点：$C_2-x\cdot C_1=M$；

[0188] 其中，C1表示所述第二密文，C2表示所述第三密文，x表示所述监管私钥，M表示所述第一坐标点。

[0189] 可选的，所述获取模块501，还用于获取由监管方公开的椭圆曲线公共参数，其中，所述椭圆曲线公共参数包括椭圆曲线的线阶n；

[0190] 所述数据处理装置还包括：

[0191] 生成模块，用于随机生成小于n的随机数x；

[0192] 所述确定模块503，还用于将所述随机数x确定为监管私钥。

[0193] 保存模块，用于保存所述监管私钥。

[0194] 可选的，所述获取模块501，还用于获取用户标识；

[0195] 所述数据处理装置还包括：

[0196] 验证模块，用于对所述用户标识进行身份验证；

[0197] 所述生成模块，还用于若所述身份验证成功，采用哈希算法，根据所述用户标识，生成待挂失数据对应的明文索引编号；

[0198] 所述获取模块501，还用于从所述区块链上，获取所述明文索引编号对应的历史密文，所述历史密文包括历史第一密文、历史第二密文和历史第三密文；

[0199] 所述计算模块502，还用于根据所述监管私钥、所述历史第二密文和所述历史第三密文，计算第二对称加密密钥映射在所述椭圆曲线上的第二坐标点；

[0200] 所述确定模块503，还用于根据所述椭圆曲线上坐标点的映射规则，确定所述第二坐标点对应的第二对称加密密钥；

[0201] 所述解密模块504，还用于利用所述第二对称加密密钥，对所述历史第一密文进行解密，获得所述待挂失数据；

[0202] 所述生成模块，还用于根据所述待挂失数据，生成隐私数据登记簿。

[0203] 在图5所描述的数据处理装置中，可以从区块链上拉取任意的密文数据，并使用监管私钥，对密文数据进行解密，获得用户的隐私数据，并对隐私数据实现监管，而其他用户，在不拥有监管私钥的前提下，是无法解开区块链上的密文数据的，从而可以保护用户的隐私数据。

[0204] 如图6所示，图6是本发明实现基于区块链的数据处理方法的较佳实施例的用户客户端的结构示意图。所述用户客户端6包括存储器61、至少一个处理器62、存储在所述存储器61中并可在所述至少一个处理器62上运行的计算机程序63及至少一条通讯总线64。

[0205] 本领域技术人员可以理解，图6所示的示意图仅仅是所述用户客户端6的示例，并不构成对所述用户客户端6的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件，例如所述用户客户端6还可以包括输入输出设备、网络接入设备等。

[0206] 所述至少一个处理器62可以是中央处理单元(Central Processing Unit,CPU)，还可以是其他通用处理器、数字信号处理器(Digital Signal Processor,DSP)、专用集成电路(Application Specific Integrated Circuit,ASIC)、现场可编程门阵列(Field-

Programmable Gate Array,FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。该处理器62可以是微处理器或者该处理器62也可以是任何常规的处理器等,所述处理器62是所述用户客户端6的控制中心,利用各种接口和线路连接整个用户客户端6的各个部分。

[0207] 所述存储器61可用于存储所述计算机程序63和/或模块/单元,所述处理器62通过运行或执行存储在所述存储器61内的计算机程序和/或模块/单元,以及调用存储在存储器61内的数据,实现所述用户客户端6的各种功能。所述存储器61可主要包括存储程序区和存储数据区,其中,存储程序区可存储操作系统、至少一个功能所需的应用程序(比如声音播放功能、图像播放功能等)等;存储数据区可存储根据用户客户端6的使用所创建的数据(比如音频数据)等。此外,存储器61可以包括非易失性存储器,例如硬盘、内存、插接式硬盘,智能存储卡(Smart Media Card,SMC),安全数字(Secure Digital,SD)卡,闪存卡(Flash Card)、至少一个磁盘存储器件、闪存器件、或其他非易失性固态存储器件。

[0208] 结合图1,所述用户客户端6中的所述存储器61存储多个指令以实现一种基于区块链的数据处理方法,所述处理器62可执行所述多个指令从而实现:

[0209] 获取待登记的隐私数据;

[0210] 随机生成对称加密密钥,并根据对称加密算法,使用所述对称加密密钥对所述隐私数据进行加密,获得第一密文;

[0211] 将所述对称加密密钥映射至公开的椭圆曲线上,获得所述椭圆曲线上的第一坐标点;

[0212] 随机生成第一随机数;

[0213] 采用非对称加密算法,根据所述第一随机数以及所述椭圆曲线的基点,计算第二密文,以及根据所述第一坐标点、所述第一随机数以及预先获取的监管公钥,计算第三密文;

[0214] 将所述第一密文、所述第二密文、所述第三密文以及所述隐私数据对应的明文索引编号发送至区块链,以将所述隐私数据保存在所述区块链上。

[0215] 在一种可选的实施方式中,在所述获取待登记的隐私数据之前,所述处理器62可执行所述多个指令从而实现:

[0216] 获取由监管方公开的椭圆曲线公共参数以及监管公钥,其中,所述椭圆曲线公共参数包括椭圆曲线的基点G和椭圆曲线的线阶n;

[0217] 所述随机生成第一随机数包括:随机生成小于n的第一随机数k;

[0218] 所述采用非对称加密算法,根据所述第一随机数以及所述椭圆曲线的基点,计算第二密文,以及根据所述第一坐标点、所述第一随机数以及预先获取的监管公钥,计算第三密文包括:

[0219] 利用如下公式计算第二密文和第三密文:$\begin{cases} C_1 = k \cdot G \\ C_2 = M + k \cdot Y \end{cases}$;其中,M表示所述第一坐标点,Y表示所述监管公钥,C1表示所述第二密文,C2表示所述第三密文。

[0220] 在一种可选的实施方式中,所述处理器62可执行所述多个指令从而实现:

[0221] 将所述第一随机数映射成密钥二维码;

[0222] 将所述密钥二维码与所述明文索引编号输出在隐私数据登记簿上。

[0223] 在一种可选的实施方式中，所述处理器62可执行所述多个指令从而实现：

[0224] 获取待查询的目标明文索引编号和目标密钥二维码；

[0225] 向所述区块链发送所述目标明文索引编号，以获取所述区块链上保存的目标密文，所述目标密文包括目标第一密文、目标第二密文和目标第三密文；

[0226] 读取所述目标密钥二维码，获得目标随机数；

[0227] 根据所述目标第三密文、所述目标随机数以及所述监管公钥，计算目标对称加密密钥映射在所述椭圆曲线上的目标坐标点；

[0228] 根据所述椭圆曲线上坐标点的映射规则，确定所述目标坐标点对应的目标对称加密密钥；

[0229] 利用所述目标对称加密密钥，对所述目标第一密文进行解密，获得目标隐私数据。

[0230] 在一种可选的实施方式中，所述将所述第一密文、所述第二密文、所述第三密文以及所述隐私数据对应的明文索引编号发送至区块链上之前，所述处理器62可执行所述多个指令从而实现：

[0231] 获取所述隐私数据所属用户的用户标识；

[0232] 采用哈希算法，根据所述用户标识，生成所述隐私数据对应的明文索引编号。

[0233] 具体地，所述处理器62对上述指令的具体实现方法可参考图1对应实施例中相关步骤的描述，在此不赘述。

[0234] 在图6所描述的用户客户端6中，可以通过对称加密密钥以及非对称加密算法对用户的隐私数据进行隐私保护处理，获得了第一密文、第二密文以及第三密文，保证了隐私数据能够以密文形式传送至区块链，同时，利用区块链上的数据具有不可篡改的性质，将密文数据发送至区块链存储，可以有效对隐私数据进行追踪记录，从而能够提供健全有效的数据记录，同时，确保数据的安全。

[0235] 如图7所示，图7是本发明实现基于区块链的数据处理方法的较佳实施例的监管客户端的结构示意图。所述监管客户端7包括存储器71、至少一个处理器72、存储在所述存储器71中并可在所述至少一个处理器72上运行的计算机程序73及至少一条通讯总线74。

[0236] 结合图3，所述监管客户端7中的所述存储器71存储多个指令以实现一种基于区块链的数据处理方法，所述处理器72可执行所述多个指令从而实现：

[0237] 从区块链上获取待监管密文，所述待监管密文包括第一密文、第二密文和第三密文；

[0238] 获取预先保存的监管私钥；

[0239] 根据所述监管私钥、所述第二密文和所述第三密文，计算第一对称加密密钥映射在椭圆曲线上的第一坐标点；

[0240] 根据所述椭圆曲线上坐标点的映射规则，确定所述第一坐标点对应的第一对称加密密钥；

[0241] 利用所述第一对称加密密钥，对所述第一密文进行解密，获得监管数据。

[0242] 在一种可选的实施方式中，所述处理器72根据所述监管私钥以及所述第二密文和所述第三密文，计算第一对称加密密钥映射在椭圆曲线上的第一坐标点包括：

[0243] 利用如下公式计算目标坐标点：$C_2-x\cdot C_1=M$；

[0244] 其中，C1表示所述第二密文，C2表示所述第三密文，x表示所述监管私钥，M表示所

述第一坐标点。

[0245] 在一种可选的实施方式中，所述从区块链上获取待监管密文之前，所述处理器72可执行所述多个指令从而实现：

[0246] 获取由监管方公开的椭圆曲线公共参数，其中，所述椭圆曲线公共参数包括椭圆曲线的线阶n；

[0247] 随机生成小于n的随机数x，并将所述随机数x确定为监管私钥；

[0248] 保存所述监管私钥。

[0249] 在一种可选的实施方式中，所述从区块链上获取待监管密文之前，所述处理器72可执行所述多个指令从而实现：

[0250] 获取用户标识；

[0251] 对所述用户标识进行身份验证；

[0252] 若所述身份验证成功，采用哈希算法，根据所述用户标识，生成待挂失数据对应的明文索引编号；

[0253] 从所述区块链上，获取所述明文索引编号对应的历史密文，所述历史密文包括历史第一密文、历史第二密文和历史第三密文；

[0254] 根据所述监管私钥、所述历史第二密文和所述历史第三密文，计算第二对称加密密钥映射在所述椭圆曲线上的第二坐标点；

[0255] 根据所述椭圆曲线上坐标点的映射规则，确定所述第二坐标点对应的第二对称加密密钥；

[0256] 利用所述第二对称加密密钥，对所述历史第一密文进行解密，获得所述待挂失数据；

[0257] 根据所述待挂失数据，生成隐私数据登记簿。

[0258] 在图7所描述的监管客户端7中，监管客户端可以从区块链上拉取任意的密文数据，并使用监管私钥，对密文数据进行解密，获得用户的隐私数据，并对隐私数据实现监管，而其他用户，在不拥有监管私钥的前提下，是无法解开区块链上的密文数据的，从而可以保护用户的隐私数据。

[0259] 所述用户客户端6/监管客户端7集成的模块/单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本发明实现上述实施例方法中的全部或部分流程，也可以通过计算机程序来指令相关的硬件来完成，所述的计算机程序可存储于一计算机可读存储介质中，该计算机程序在被处理器执行时，可实现上述各个方法实施例的步骤。其中，所述计算机程序包括计算机程序代码，所述计算机程序代码可以为源代码形式、对象代码形式、可执行文件或某些中间形式等。所述计算机可读介质可以包括：能够携带所述计算机程序代码的任何实体或装置、记录介质、U盘、移动硬盘、磁碟、光盘、计算机存储器以及只读存储器(ROM，Read-Only Memory)。

[0260] 在本发明所提供的几个实施例中，应该理解到，所揭露的系统，装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述模块的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式。

[0261] 所述作为分离部件说明的模块可以是或者也可以不是物理上分开的，作为模块显

示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本实施例方案的目的。

[0262] 另外，在本发明各个实施例中的各功能模块可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用硬件加软件功能模块的形式实现。

[0263] 对于本领域技术人员而言，显然本发明不限于上述示范性实施例的细节，而且在不背离本发明的精神或基本特征的情况下，能够以其他的具体形式实现本发明。因此，无论从哪一点来看，均应将实施例看作是示范性的，而且是非限制性的，本发明的范围由所附权利要求而不是上述说明限定，因此旨在将落在权利要求的等同要件的含义和范围内的所有变化涵括在本发明内。不应将权利要求中的任何附关联图标记视为限制所涉及的权利要求。系统权利要求中陈述的多个单元或装置也可以由一个单元或装置通过软件或者硬件来实现。

[0264] 最后应说明的是，以上实施例仅用以说明本发明的技术方案而非限制，尽管参照较佳实施例对本发明进行了详细说明，本领域的普通技术人员应当理解，可以对本发明的技术方案进行修改或等同替换，而不脱离本发明技术方案的精神和范围。

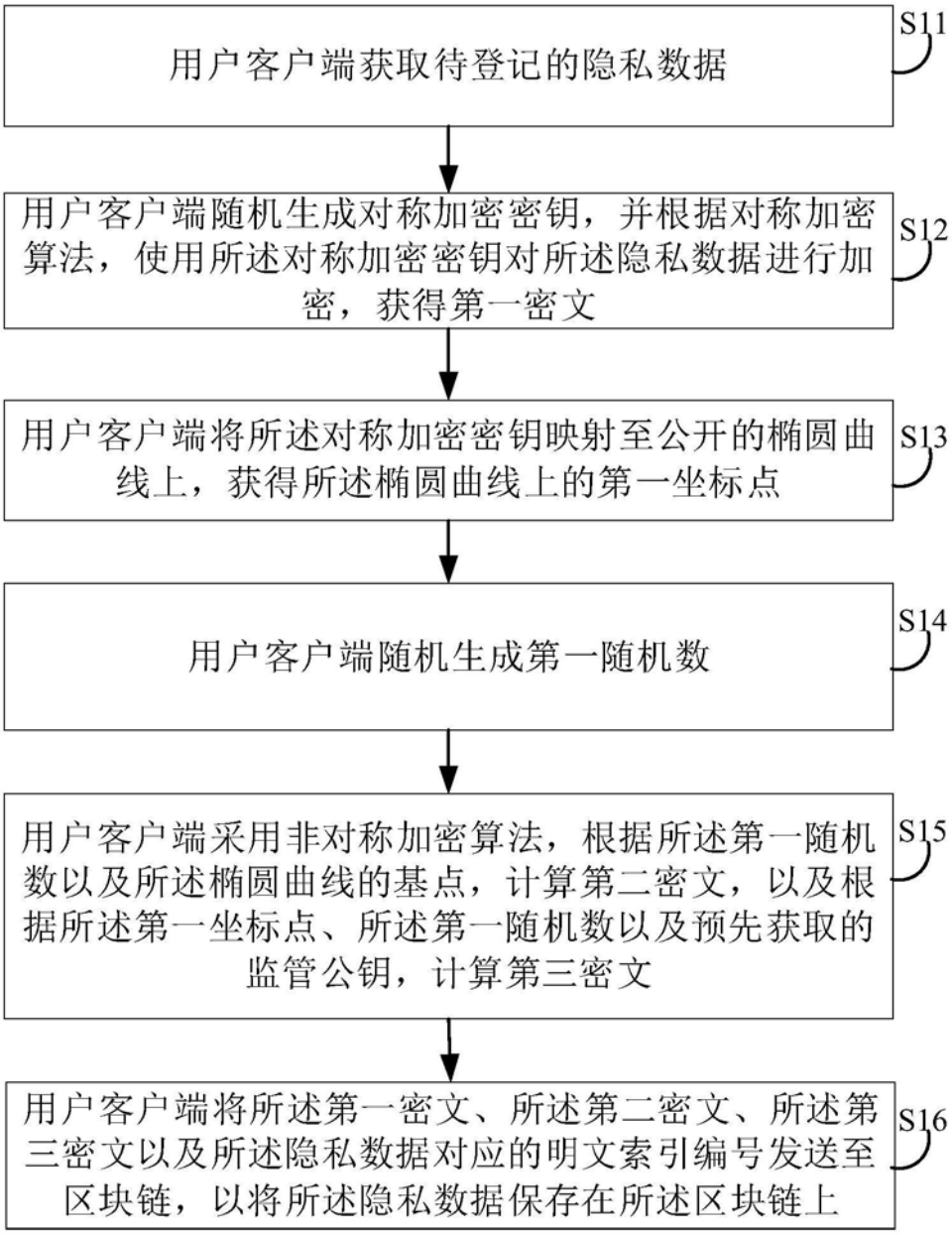

用户客户端获取待登记的隐私数据
S11
用户客户端随机生成对称加密密钥，并根据对称加密算法，使用所述对称加密密钥对所述隐私数据进行加密，获得第一密文
S12
用户客户端将所述对称加密密钥映射至公开的椭圆曲线上，获得所述椭圆曲线上的第一坐标点
S13
用户客户端随机生成第一随机数
S14
用户客户端采用非对称加密算法，根据所述第一随机数以及所述椭圆曲线的基点，计算第二密文，以及根据所述第一坐标点、所述第一随机数以及预先获取的监管公钥，计算第三密文
S15
用户客户端将所述第一密文、所述第二密文、所述第三密文以及所述隐私数据对应的明文索引编号发送至区块链，以将所述隐私数据保存在所述区块链上
S16

图1


疫苗接种本
姓名：张三 身份证号：XXXXXXXXXXXXXXXXXX
链上编号 疫苗类型 接种日期 地点编号 疫苗批次 密钥二维码
XXXX 0001 20190425 0001 XXXXXX
XXXX 0012 20190517 0001 XXXXXX

图2

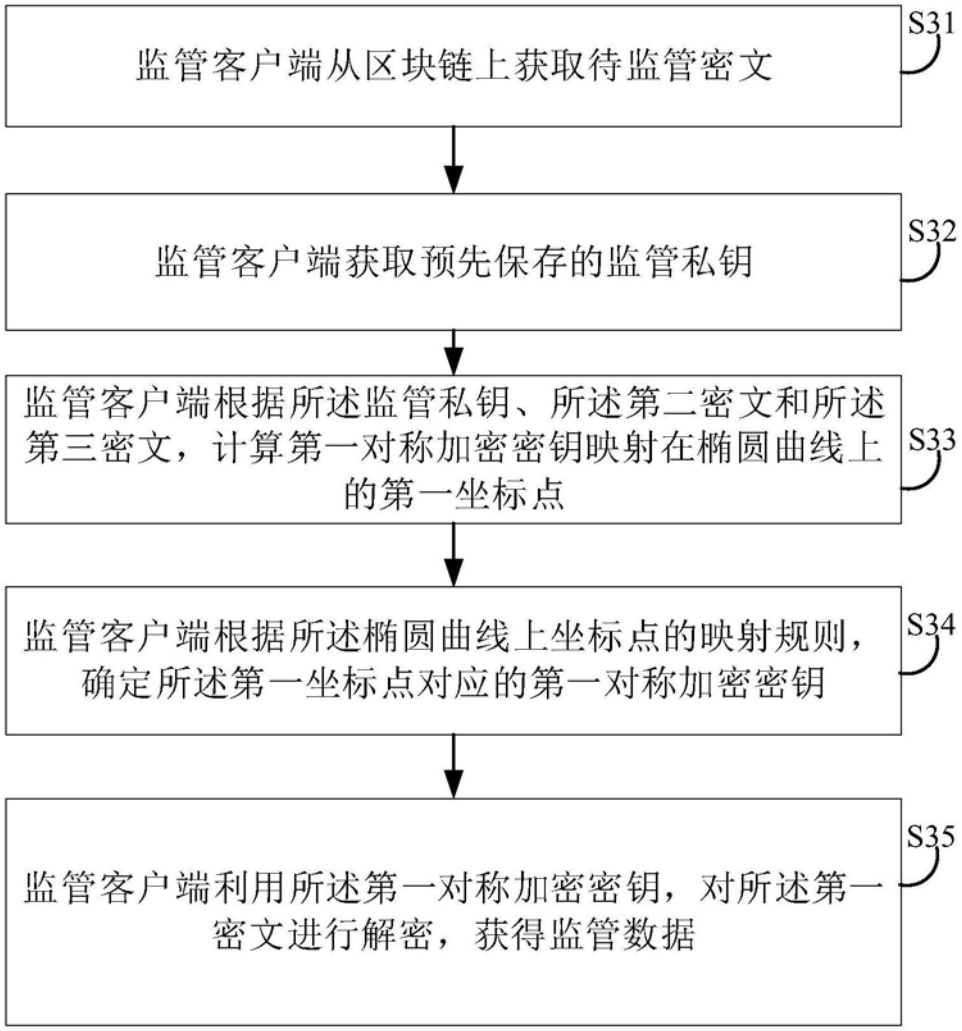

监管客户端从区块链上获取待监管密文
S31
监管客户端获取预先保存的监管私钥
S32
监管客户端根据所述监管私钥、所述第二密文和所述第三密文，计算第一对称加密密钥映射在椭圆曲线上的第一坐标点
S33
监管客户端根据所述椭圆曲线上坐标点的映射规则，确定所述第一坐标点对应的第一对称加密密钥
S34
监管客户端利用所述第一对称加密密钥，对所述第一密文进行解密，获得监管数据
S35

图3

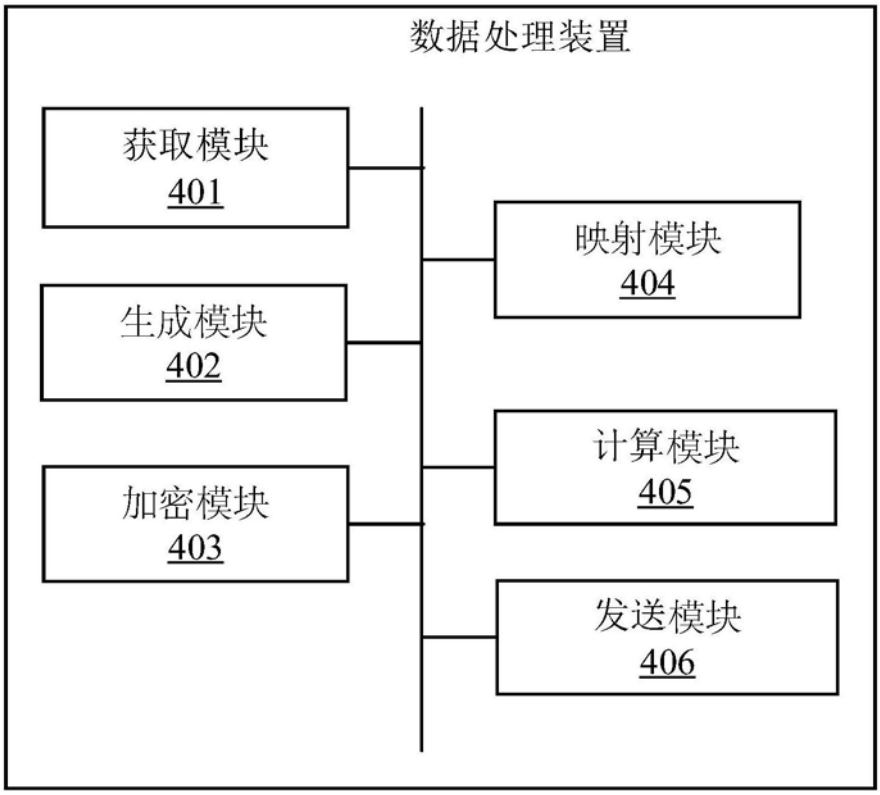

数据处理装置
获取模块
401
生成模块
402
加密模块
403
映射模块
404
计算模块
405
发送模块
406

图4

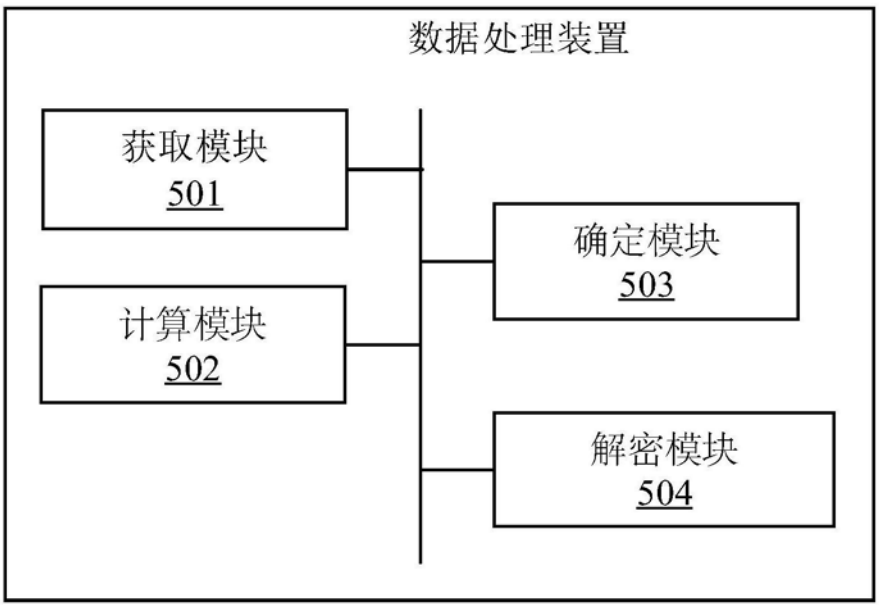

数据处理装置
获取模块
501
计算模块
502
确定模块
503
解密模块
504

图5

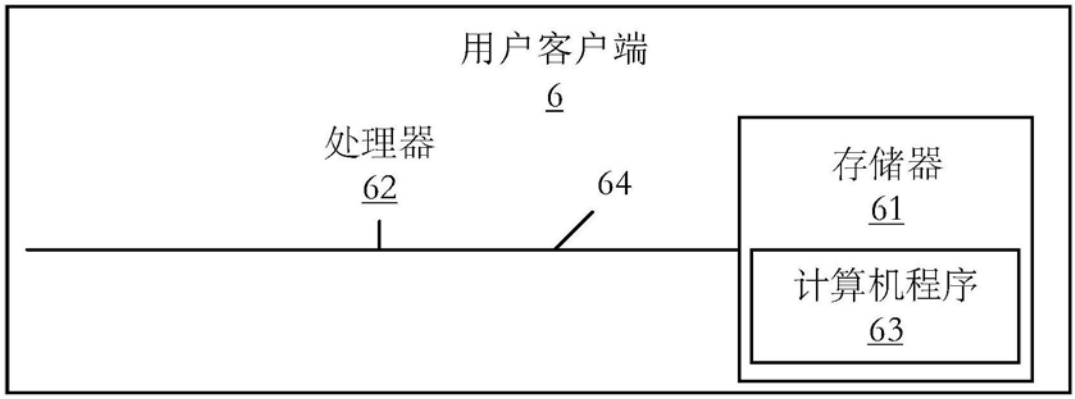

用户客户端
6
处理器
62
64
存储器
61
计算机程序
63

图6

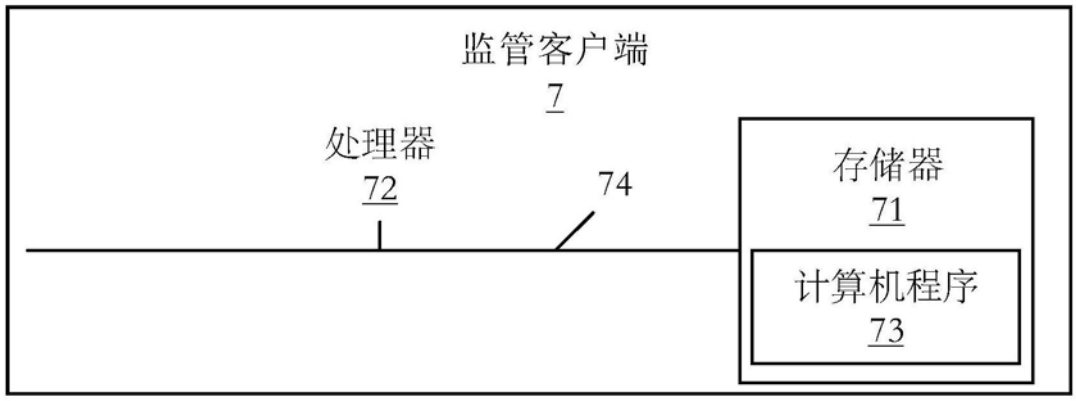

监管客户端
7
处理器
72
74
存储器
71
计算机程序
73

图7