(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 109388960 A
(43)申请公布日 2019.02.26

(21)申请号 201811237887.0

(22)申请日 2018.10.24

(71)申请人 全链通有限公司
地址 100043 北京市石景山区实兴东街11号5层5158室

(72)发明人 路成业 王凌 王童

(51)Int.Cl.
G06F 21/60(2013.01)
G06F 21/62(2013.01)

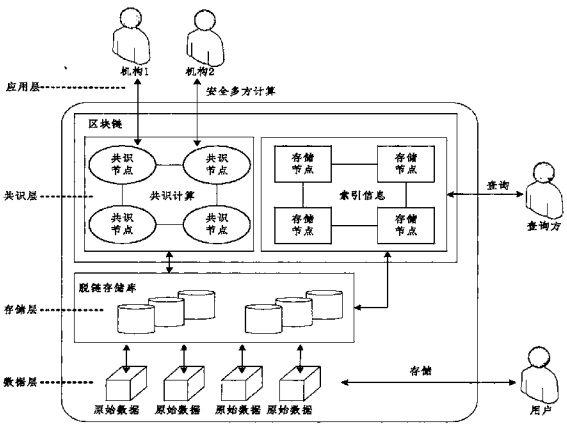
权利要求书2页 说明书5页 附图3页

(54)发明名称

基于区块链的信息共享及安全多方计算模型

(57)摘要

本发明公开了一种基于区块链的信息共享及安全多方计算协议，主要解决现有安全多方计算容易造成用户不能自主控制数据即易被第三方获取数据的问题，提出的技术方案为：1)构建存储模型，将链上索引表信息与链下数据库相结合的方式进行存储。2)构建数据共享模型，用户可以通过授权第三方访问其数据，也可以随时收回权限。3)利用区块链的共识机制保证节点间的一致性；4)在节点正确性的基础上，利用MapReduce编程模型，将模型分为Map和Reduce两个阶段，主节点对节点进行Map和Reduce的任务分配；5)Map节点利用改进的同态加密算法进行加密计算；6)Reduce节点将加密后的数据进行整合输出数据文件。



CN 109388960 A

1.基于区块链的信息共享及安全多方计算模型,包括:

1)构建区块链的存储模型:

采用链上索引表信息与链下数据库相结合的方式进行存储。链上的索引表存储索引信息(索引类别及加密文件的地址),并形成索引区块存放在区块链上。索引表将查询者查询的信息类别与存储地址值相对应,在链上占用少部分内存。链下的数据库存储数据拥有者上传的加密数据文件,保证数据的安全性。

2)构建数据共享模型:

用户可以通过授权第三方访问其数据,也可以随时收回权限,撤销第三方对数据的访问。

3)构建区块链的共识算法模型:

3a)共识系统由n个共识节点组成,提供f=(n-1)/3的容错能力。节点同步过程采用向其他节点索要区块并校验的方式完成同步。

3b)视图更换过程是在结合区块生成协议的基础上,再采用超时机制进行试图切换。在一定程度上减少算力开销和数据传输量。

4)构建安全多方计算模型:

4a)利用MapReduce编程模型,将模型分为Map和Reduce两个阶段,主节点对节点进行Map和Reduce的任务分配。

4b)将原始数据文件切割分片为几个小的文件,交给Map节点进行并行处理,Map节点将数据进行安全多方计算,将经过改进的同态加密算法加密运算后的结果交给Reduce节点进行整合得到最后的输出数据文件。

2.根据权利要求1所述的方法,其中步骤1)为为了保持对加密数据的访问,利用链下分布式哈希存储,按如下步骤进行:

2a)数据拥有者将上传数据进行分类(t1,t2...),返回数据类别

2b)将不同类别的数据用公钥进行加密,存储至链下数据库

2c)将不同类别信息存储的地址值返回至链上,创建索引表。

3.根据权利要求1所述的方法,其中步骤2)中为了使用户对数据的使用权限完全由用户自己控制数据共享模型,按如下进行:信息共享时,如果查询者想要查询相关数据信息,查询者可以向区块链发出信息查询请求,在通过授权后可以通过索引表中的地址值在链下数据库中进行查找加密文件,利用用户私钥和查询者公钥生成的重加密密钥对加密文件二次加密返回至查询者,用查询者的私钥进行解密获得信息。

4.根据权利要求1所述的方法,其中步骤3a)中的节点同步过程,按如下步骤进行:

4a)用户发起一笔交易时,利用私钥签名后,向全网进行广播。当节点收到一笔交易后,判断是否为主节点,若为主节点,则主节点经过时间t发送共识提案

4b)其他从节点在收到主节点发送过来的共识提案后,对提案检查为真后,向出自己之外的从节点及其主节点发送共识确认消息。

5.根据权利要求1所述的方法,其中步骤3b)中如果从节点怀疑主节点,广播发送视图更换信息,进行视图更换,按如下步骤进行:

5a)令k=1,v_k=v+k

其中,v表示视图的编号,v_k表示视图编号的大小

5b)节点i发出的视图更换请求为<changeview,h,v,i,vk>

其中,h表示区块的高度,

5c)任意节点收到至少n-f个来自不同i的相同v_k后,视图更换达成,令v=v_k开始共识

5d)如果在$2^{v_k+1}\cdot t$时间间隔后,视图仍未达成,则k递增并返回到第3b步。

6.根据权利要求1所述的方法,其中步骤4b)中为了获得密文长度小,公钥尺寸相对小的密文,进行同态加密算法的改进,按如下步骤进行:

4a)密钥生成算法:随机产生一个比特的素数p,$p\in[2^{\eta-1},2^{\eta})$,令$x_0=q_0\cdot p$,$q_0$是$[0,2^{\gamma}/p)$里的奇整数。产生整数$x_{i,b}=p\cdot q_{i,b}+2^k\cdot r_{i,b}$,其中$q_{i,b}$是随机整数,$r_{i,b}$是$(-2^{\rho},2^{\rho})$中的整数,令密钥sk=p,$pk=(x_0,x_{1,0},x_{1,1},x_{1,2},\ldots,x_{\beta,0}x_{\beta,1}x_{\beta,2})$

4b)加密算法:随机产生一个尺寸为$\tau=\beta^3$的向量$b=(b_{i,j,k})$,向量系数在$[0,2^{\alpha})$产生一随机整数$r\in(-2^{\rho'},2^{\rho'})$,输出密文为$c=m+2^k r+2^k\sum_{1\le i,j,k\le\beta} b_{i,j,k}\cdot x_{i,0}\cdot x_{j,1}\cdot x_{k,2} \bmod x_0$

4c)评估算法:给定二进制t输出的电路C,t个密文C_i将C中的加法和乘法门电路用于密文操作,所有操作在整数上执行,返回结果为整数

4d)解密算法:输出$m\leftarrow(c \bmod p)\bmod 2^k$。

基于区块链的信息共享及安全多方计算模型

技术领域

[0001] 本发明属于信息安全技术领域，涉及一种基于区块链的共享及安全多方计算 模型。

背景技术

[0002] 随着当今社会迅速发展，数字化和信息化的程度越来越高，数据隐私对生活 和工作产生很大的影响，在医疗健康，金融等领域，数据隐私保护已成为重中之 重。不同于传统系统的中心化他信机制，区块链技术具有去可信第三方的共信特 性，使用户可以自己控制自己的数据。区块链的数据对所有人公开，任何人都可 以通过公开的接口查询数据，整个系统信息高度透明。因此区块链作为一个分布 式可验证的账本，可以构建可行安全计算平台的基础。

[0003] 安全多方计算指在一个分布式网络中，多个用户各自持有一些数据输入，希 望共同完成对数据的计算，同时要求每个用户除计算结果外均不能获知其他用户 的任何输入信息。单纯的使用安全多方计算在一定程度上不会泄露用户的隐私，但是用户不能自主控制数据，第三方机构很有可能因自己利益获取数据。因此区 块链和安全多方计算二者相结合，既保护了隐私，同时也使用户拥有对数据的控 制权。

[0004] 但是区块链去中心化的特点决定了任何一个参与者都不能被信任，可能会出 现恶意节点以及因各方利益不一致导致的数据分歧等问题。和任何分布式系统一 样，区块链系统会面临网络延迟，安全漏洞等问题。而且现有的高性能计算多采 用集中共享式存储系统，这种以存储为中心的体系结构简化程序编写的复杂度，在处理大规模数据时，易降低系统整体性能，平均无故障时间缩短，系统可用性 下降。如何解决节点间相互信任的问题并在相互信任的基础上利用高性能计算实 现安全多方计算是需要解决的技术问题。

发明内容

[0005] 本发明的目的在于提出一种基于区块链的信息共享及安全多方计算模型，通 过区块链与安全多方计算相结合的方法，来解决传统安全多方计算使用户不能自 主控制数据，第三方机构很有可能因自己利益获取数据的问题。

[0006] 本发明的技术思路是：通共识机制对区块链中各个节点，在区块链上先利用 共识机制解决区块链节点间相互信任的问题。在相互信任的基础上，利用安全多 方计算各节点共同计算出需要得到的函数值，即采用MapReduce并行框架模型 将用户的输入利用改进的同态加密算法进行计算，并将结果返回给用户，在此过 程中不会泄露任何隐私信息。用户生成新的加密密钥进行数据的加密，存储在 链下进行保存，并根据使用者的请求进行访问数据权限的授予。

[0007] 根据上述思路，本发明的实现步骤包括如下：

[0008] 1)构建区块链的存储模型：

[0009] 采用链上索引表信息与链下数据库相结合的方式进行存储。链上的索引表 存储

索引信息(索引类别及加密文件的地址),并形成索引区块存放在区块链上。索引表将查询者查询的信息类别与存储地址值相对应,在链上占用少部分内存。链下的数据库存储数据拥有者上传的加密数据文件,保证数据的安全性。

[0010] 2)构建数据共享模型:

[0011] 用户可以通过授权第三方访问其数据,也可以随时收回权限,撤销第三方 对数据的访问。

[0012] 3)构建区块链的共识算法模型:

[0013] 3a)共识系统由n个共识节点组成,提供f=(n-1)/3的容错能力。节点同步 过程采用向其他节点索要区块并校验的方式完成同步。

[0014] 3b)视图更换过程是在结合区块生成协议的基础上,再采用超时机制进行 试图切换。在一定程度上减少算力开销和数据传输量。

[0015] 4)构建安全多方计算模型:

[0016] 4a)利用MapReduce编程模型,将模型分为Map和Reduce两个阶段,主 节点对节点进行Map和Reduce的任务分配。

[0017] 4b)将原始数据文件切割分片为几个小的文件,交给Map节点进行并行处 理,Map节点将数据进行安全多方计算,将经过改进的同态加密算法加密运算 后的结果交给Reduce节点进行整合得到最后的输出数据文件。

[0018] 本发明与现有技术相比具有以下优点:

[0019] 本发明通过利用区块链去中心化的特点,将用户的公共信息保存在区块链上 无法被篡改,在利用共识机制确保节点的正确性和安全性的前提下,区块链分布 式的结构使得数据分散在不同的节点,不易受到攻击,单点威胁不会影响到整个 网络。利用区块链用户可以自主控制数据,且第三方机构不能因自己利益获取数 据。

[0020] 本发明通过改进的同态加密算法,用户输入的数据进行处理时,利用改进 的同态加密算法可以得到相对较小的密文长度和公钥尺寸,在数据量特别大的时 候,更适合大数据的处理。利用MapReduce编程模型可以并行处理数据,在大 数据处理中处理速度更快。

附图说明

[0021] 图1是数据存储及共享流程图;

[0022] 图2是本发明种共识模型中的共识算法流程图;

[0023] 图3是本发明中MapReduce框架流程;

[0024] 图4是本发明中区块链上的节点参与安全计算的流程图;

[0025] 图5是两种安全多方计算的安全性分析对比图;

图6是基于区块链的信息共享隐私保护框架模型图;

具体实施方式

[0026] 本发明的实现步骤如下:

[0027] 步骤1,构建链下数据存储模型

[0028] 本步骤将敏感的信息及数据量较大的信息在链下进行存储,链上存储用户及 文档的索引信息及数据量较小的信息。不论是用户本身还是需要使用数据的机构, 都不能随

意更改数据，由此保证了数据的安全性。

[0029] 用户对要上传的文件信息进行分类，如商业信息，医疗信息等，并对外公布 分类，然后将对应分类中的数据用公钥进行加密并存储到链下数据库中形成加密 文件，之后将存储的地址值返回至链上存储在索引表中。如图1所示，具体步骤 如下：

[0030] 1a)数据拥有者将上传数据进行分类(t1，t2...)，返回数据类别

[0031] 1b)将不同类别的数据用公钥进行加密，存储至链下数据库

[0032] 1c)将不同类别信息存储的地址值返回至链上，创建索引表

[0033] 步骤2，构建数据共享模型

[0034] 以医疗场景为例，病人对数据的使用权限完全由用户自己控制，病人可以通 过授权第三方访问其医疗记录，也可以随时收回权限，撤销第三方对医疗记录的 访问。

[0035] 信息共享时，如果查询者想要查询相关数据信息，查询者可以向区块链发出 信息查询请求，在通过授权后可以通过索引表中的地址值在链下数据库中进行查 找加密文件，利用用户私钥和查询者公钥生成的重加密密钥对加密文件二次加密 返回至查询者，用查询者的私钥进行解密获得信息。

[0036] 步骤3，构建区块链的共识模型。

[0037] 本步骤在进行安全多方计算之前，先进行节点间的共识确定节点的正确性， 如图2所示，分为如下两步进行：

[0038] 3a)节点同步过程采用向其他节点索要区块并校验的方式完成同步，节点同 步过程如图3所示，步骤如下：

[0039] 3a1)用户发起一笔交易时，利用私钥签名后，向全网进行广播。当节点收 到一笔交易后，判断是否为主节点。若不是主节点，则转发即可。若为主节点， 则需要验证交易的合法性，若为合法的，则存入内存中，记录到区块数据结构的 交易字段中，若不合法，直接丢弃。

[0040] 3a2)主节点经过时间t发送共识提案<PrepareRequest，h，v，P，block，<block>>，其他从节点在收到主节点发送过来的共识提案后，对提案检查为真后，向出自己 之外的从节点及其主节点发送共识确认消息 <PrepareResponse，h，v，i，block，<block>>

[0041] 3b)若检查提案后发现不为真，则从节点怀疑主节点，广播发送视图更换信 息。视图更换过程如图2所示，步骤如下：

[0042] 3b1)令k＝1，v_k＝v，+k

[0043] 其中，v表示视图的编号，v_k表示视图编号的大小

[0044] 3b2)节点i发出的视图更换请求为<changeview，h，v，i，vk>

[0045] 其中，h表示区块的高度，

[0046] 3b3)任意节点收到至少n-f个来自不同i的相同v_k后，视图更换达成，令 v＝v_k开始共识

[0047] 3b4)如果在$2^{v_k+1}\cdot t$时间间隔后，视图仍未达成，则k递增并返回到第3b2步

[0048] 3b5)网络中任意节点在收到2f个相同的确认消息后，即认为共识达成，可 以发布来自主节点的区块block，其余节点在收到block后，认为该轮共识任务 完成，将自己内存在区块里的交易删除掉，开始下一轮共识。

[0049] 步骤4，对区块链中节点进行正确验证之后，在MapReduce模型的基础上 利用改进

的同态加密算法对进行安全多方计算模型的构建。

[0050] MapReduce计算框架是一种运行在集群节点上的能处理海量数据的并行编 程模型和框架，本步骤使用并行MapReduce模型进行同态加密，如图4所示， 其过程如下：

[0051] 4a)主节点对节点进行Map和Reduce的任务分配。首先将原始输入数据文 件切割分片为几个小文件，交给Map节点进行并行处理，Map节点将数据进行 同态加密运算

[0052] 4b)基于MapReduce计算框架，在原有Somewhat同态方案基础上，构造一 个整数 $x'_{i,j,k}=x_{i,0}\cdot x_{j,1}\cdot x_{k,2} \bmod x_0$，这样为产生 $\tau=\beta^3$ 个 $x'_{i,j,k}$ 用来加密，只需在 公钥中存储3β个 $x_{i,b}$，公钥尺寸也就从τ下降至 $\sqrt[3]{\tau}$，并且该算法模2运算改成 模 2^k 运算，改进后的算法可以一次加密k bit

[0053] 其中τ是公钥的个数，η是私钥的比特长度，ρ是噪声的比特长度，

[0054] 4b1)密钥生成算法：随机产生一个比特的素数p，$p\in[2^{\eta-1},2^{\eta})$，令 $x_0=q_0\cdot p$， q_0 是 $[0,2^{\gamma}/p)$ 里的奇整数。产生整数 $x_{i,b}=p\cdot q_{i,b}+2^k\cdot r_{i,b}$，且 $1\leqslant i\leqslant\beta$，$0\leqslant b\leqslant 2$

[0055] 其中 $q_{i,b}$ 是 $c=m+2^k r+2^k\sum_{1\leq i,j,k\leq\beta} b_{i,j,k}\cdot x_{i,0}\cdot x_{j,1}\cdot x_{k,2}+kx_0$ 的随机整数，$r_{i,b}$ 是 $(-2^{\rho},2^{\rho})$ 中的整数，令密钥 $sk=p$，$pk=(x_0,x_{1,0},x_{1,1},x_{1,2},\ldots,x_{\beta,0}x_{\beta,1}x_{\beta,2})$

[0056] 4b2)加密算法：随机产生一个尺寸为 $\tau=\beta^3$ 的向量 $b=(b_{i,j,k})$，向量系数在 $[0,2^{\alpha})$ 产生一随机整数 $r\in(-2^{\rho'},2^{\rho'})$，输出密文为

[0057] $$c=m+2^k r+2^k\sum_{1\leq i,j,k\leq\beta} b_{i,j,k}\cdot x_{i,0}\cdot x_{j,1}\cdot x_{k,2} \bmod x_0$$

[0058] 4b3)评估算法：给定二进制t输出的电路C，t个密文 C_i 将C中的加法和乘法 门电路用于密文操作，所有操作在整数上执行，返回结果为整数

[0059] 4b4)解密算法：输出 $m\leftarrow(c \bmod p) \bmod 2^k$

[0060] 4c)将使用安全多方计算后的加密运算结果交给Reduce节点进行整合得到 最后的输出数据，然后传递给用户

[0061] 如果对单个比特进行加密，而且公钥中分量形式为线性，所以加密得到的密 文会很大。本发明加密明文比特数为k比特，且公钥中分量的形式采用三次，使 密文长度变小，公钥尺寸相对变小，在数据量特别大的时候，更适合大数据的处 理。

[0062] 本发明的优点可以通过图5的安全性对比图进行说明：

[0063] 传统的安全多方计算可能存在参与方共谋篡改数据的安全隐患。以区块链作 为安全多方计算的基础，在同态加密计算之前，节点同步过程采用向其他节点索 要区块并校验的方式完成同步，共同确认一个节点的正确性，进而才能进行同态 加密计算，保证交易的安全性。

[0064] 用户的公共数据都存储在区块链上，由于区块链是公开的账本，公共信息公 开无法篡改，保证了存储的安全性。当数据加密后则存储在链下，由于用户对数 据具有控制权，敌人即使从存储中获得数据，由于存储记录的是密文，因此也无 法获得真实的数据信息，从而确保数据的安全。

[0065] 用户不依赖于可信的第三方，结合安全多方计算，用户可以自主控制自己的 数据信息，具有对数据的所有权，并且在数据的产生和使用过程中都是安全的。 用户可以同意数据使用者对自己数据进行访问，也可以撤销其访问权。信息本身 被加密保存在链下，只

有用户通过使用者的访问请求,才可以解密出明文信息获 得真实数据。

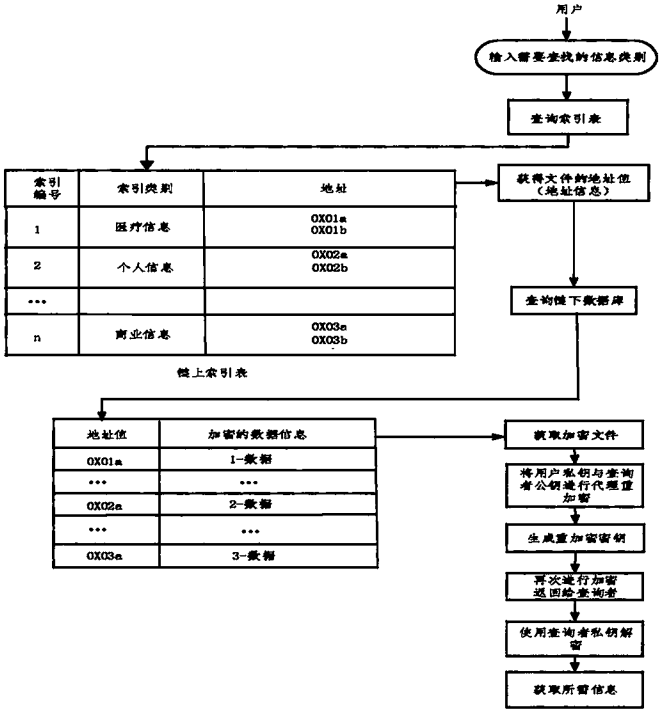

用户
输入需要查找的信息类别
查询索引表
索引编号
索引类别
地址
1
医疗信息
0X01a
0X01b
2
个人信息
0X02a
0X02b
...
n
商业信息
0X03a
0X03b
链上索引表
获得文件的地址值（地址信息）
查询链下数据库
地址值
加密的数据信息
0X01a
1-数据
0X02a
2-数据
0X03a
3-数据
获取加密文件
将用户私钥与查询者公钥进行代理重加密
生成重加密密钥
再次进行加密返回给查询者
使用查询者私钥解密
获取所需信息

图1

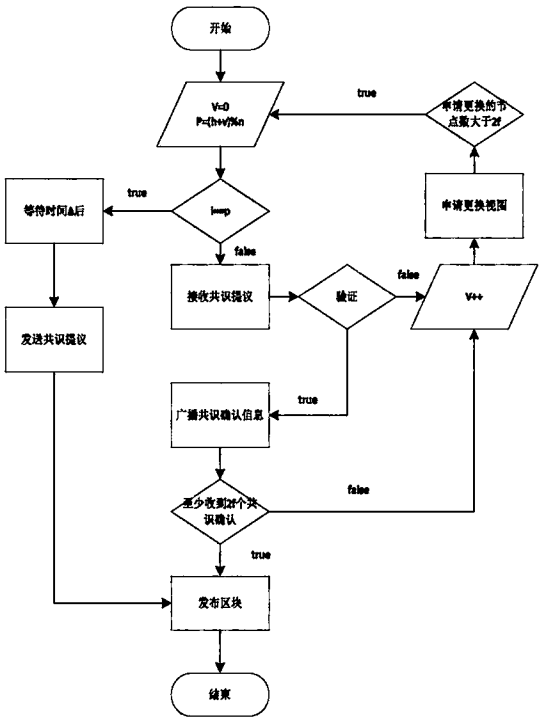

开始
V=0
P=(h+v)%n
true
申请更换的节点数大于2f
等待时间Δt后
true
loop
false
申请更换视图
接收共识提议
验证
false
V++
发送共识提议
true
广播共识确认信息
至少收到2f个共识确认
false
true
发布区块
结束

图2

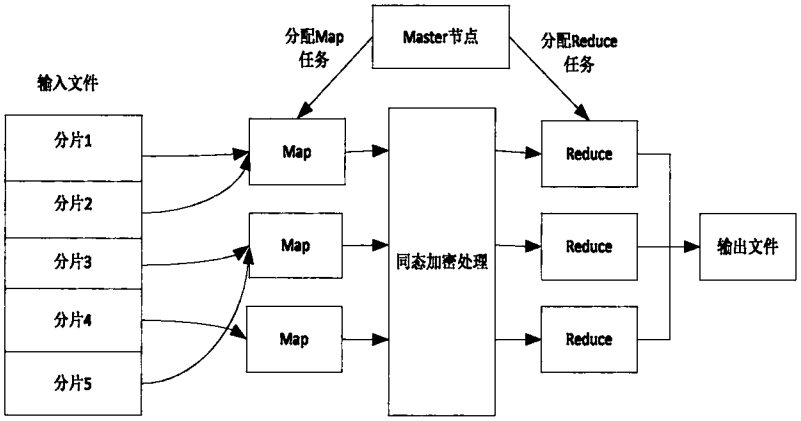


图3

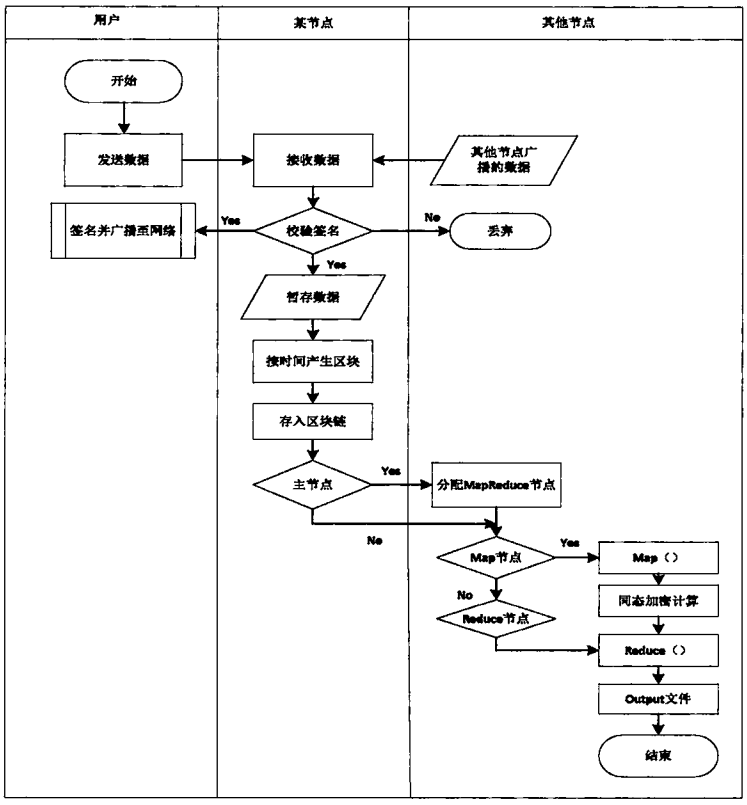


图4

	依赖可信第三方	交易验证	安全存储	用户控制权	隐私保护
现有的安全多方计算	√	×	×	×	√
基于区块链的安全多方计算	×	√	√	√	√

图5

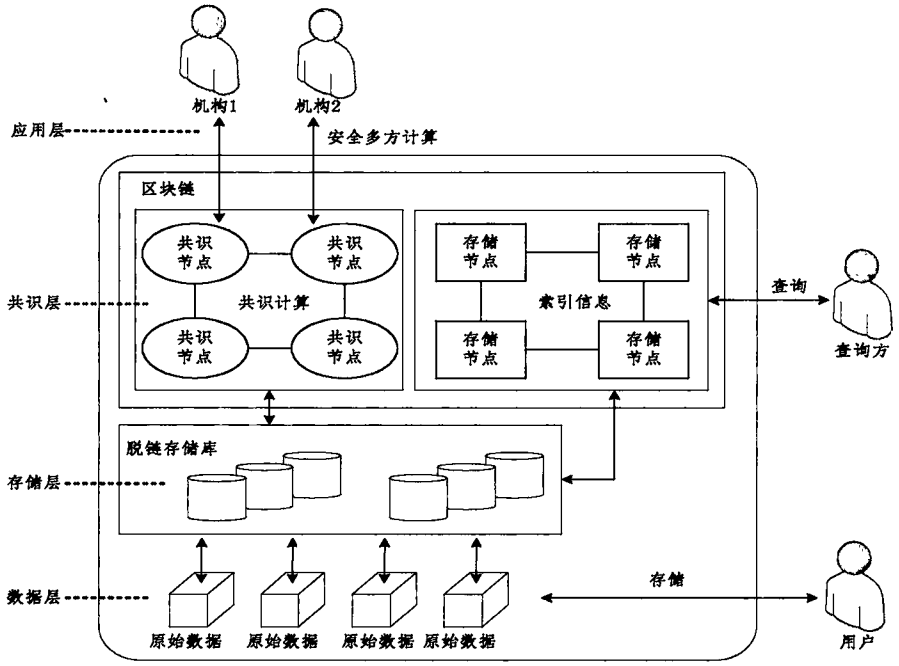

机构1
机构2
应用层
安全多方计算
区块链
共识节点
共识节点
共识节点
共识节点
共识层
共识计算
存储节点
存储节点
存储节点
存储节点
索引信息
查询
查询方
脱链存储库
存储层
数据层
存储
用户
原始数据
原始数据
原始数据
原始数据

图6