(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 113609502 A
(43)申请公布日 2021.11.05

(21)申请号 202110902314.0

(22)申请日 2021.08.06

(71)申请人 东北大学
地址 110819 辽宁省沈阳市和平区文化路3号巷11号

(72)发明人 张亚男 刘园 杜妍

(74)专利代理机构 沈阳东大知识产权代理有限公司 21109
代理人 李在川

(51)Int.Cl.
G06F 21/60(2013.01)
G06F 21/62(2013.01)
G06F 21/64(2013.01)

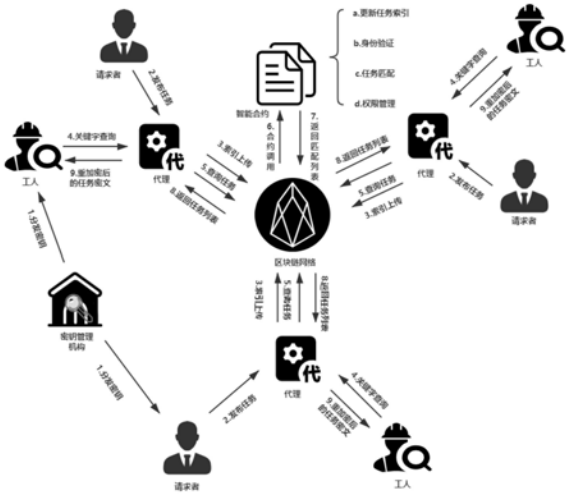
权利要求书4页 说明书8页 附图2页

(54)发明名称

一种基于区块链的空间众包系统及方法

(57)摘要

本发明公开一种基于区块链的空间众包系统及方法，系统包括用户、密钥管理机构、代理、区块链网络和智能合约。任务请求者将加密后的任务位置信息和关键字密文进行上传，工人查询任务时，提交搜索的兴趣陷门和可接受任何的距离范围，代理调用智能合约先对关键字密文进行匹配，后对任务位置转换后的密文与工人可接受的任务范围的字符串集合进行匹配，匹配成功后代理使用转换密钥进行重加密，对任务信息进行转换并发送给工人，工人得到任务密文利用工人私钥进行解密，查看任务信息。本发明使用区块链技术，既能实现请求者和工人任务在密文条件下进行匹配，又能保护用户隐私，监督众包平台的行为，从而保证了信息的透明性。



CN 113609502 A

1.一种基于区块链的空间众包系统,其特征在于,系统包括用户、密钥管理机构、代理、区块链网络和智能合约;

所述密钥管理机构接收用户的注册申请,给用户发送个人公私钥以及单独密钥;并生成转换密钥,以{用户,转换密钥}的形式发送给代理进行管理;

所述用户分为任务请求者和工人两种身份,所有用户能够在两种身份中切换角色;所述用户使用个人公私钥以及单独密钥给代理,由代理调用智能合约进行匹配;

所述任务请求者使用自己的公私钥中的公钥加密任务信息,使用单独密钥加密任务坐标以及任务的关键词;

所述工人使用自己的私钥解密经过代理重加密后的匹配到的任务密文得到任务信息,使用单独密钥加密自己的兴趣关键词以及接受的任务范围生成陷门,用来进行任务匹配;

所述代理负责用户与区块链网络的交互,并提供相关的计算匹配服务;

所述智能合约通过代理的调用情况,实现更新索引、代理重加密、任务匹配和维护授权列表的功能。

2.根据权利要求1所述的基于区块链的空间众包系统,其特征在于:所述任务请求者根据需要授权工人访问自己的任务信息。

3.采用上述权利要求1或2所述的基于区块链的空间众包系统进行隐私保护的众包方法,其特征在于,包括如下步骤:

步骤1:用户向密钥管理机构进行注册,由密钥管理机构为任务请求者和工人生成个人公私钥PK和SK、单独密钥qk以及转换密钥rk;

步骤2:由任务请求者发布任务,同时使用任务请求者的公钥PKr加密任务信息,单独密钥qk_r加密任务位置坐标以及任务的关键词;

步骤3:代理收到任务请求者发送的任务相关的密文信息,为其生成相应的任务号t_i,将任务号以及对应的加密任务的关键词和任务位置坐标创建为任务索引上传到区块链网络;

步骤4:工人使用自己的单独密钥加密自己的兴趣关键词以及接受的任务范围生成两个搜索陷门,并且上传到代理;

步骤5:代理先分别对任务位置坐标密文和工人接受任务范围的坐标进行重加密,然后代理调用匹配的智能合约将陷门与任务索引中的任务的关键词和任务位置坐标的密文进行匹配,将得到的结果返回给代理;

步骤6:代理根据匹配到的任务,查询授权列表,查看工人是否在该任务请求者的授权列表中,如果不在,则向任务请求者申请,然后更新任务请求者的授权列表;并通过重加密转换密钥将所有匹配的任务的密文进行转换,将最终得到的转换后的任务密文发送给工人;

步骤7:工人得到所有任务的密文后,进行解密操作得到任务信息明文。

4.根据权利要求3所述的采用基于区块链的空间众包系统进行隐私保护的众包方法,其特征在于,所述个人公私钥中的公钥PK为公开状态,私钥SK为用户私有状态,不可公开;任务请求者的个人公私钥对记为(PK_r,SK_r),工人的个人公私钥对记为(PK_w,SK_w);

所述公钥PK的生成过程为:

S1、用伪随机数生成器生成两个素数p和q,并将这两个素数相乘得到N:N=p*q;

S2、求解p-1和q-1的最小公倍数L:L=lcm(p-1,q-1);

S3、在(1,L)范围内通过伪随机数生成E,判断gcd(E,L)＝1是否成立,若成立则将得到的E和N作为公钥(E,N),设为PK;

所述私钥SK的生成过程为:在(1,L)范围内取D,同时使D满足E*D mod L＝1的条件,将得到的D和N作为私钥(D,N),设为SK。

5.根据权利要求4所述的采用基于区块链的空间众包系统进行隐私保护的众包方法,其特征在于,所述任务请求者使用单独密钥qk_r加密任务位置坐标以及任务的关键词;所述工人使用单独密钥qk_w加密自己的兴趣关键词以及接受的任务范围生成搜索陷门,用来进行任务匹配;所述转换密钥rk由密钥管理机构以{用户,转换密钥}的形式发送给代理进行管理,用于任务匹配时进行重加密;所述任务请求者和工人对应的转换密钥分别为rk_r和rk_w;

所述单独密钥qk和转换密钥rk的生成过程为:

S1:密钥管理机构生成随机数大质数g,生成一个公共哈希函数H,以及bigInteger类型的主密钥MSK:$(1\lambda)\rightarrow(g,H,MSK)$;

S2:对于一个用户u_i,密钥管理机构首先选择一个随机值k_i并且计算g^{ki}作为用户u_i的单独密钥qk_i,计算$rk_i=MSK/k_i$作为用户u_i的转换密钥rk_i:$(MSK,u_i)\rightarrow(qk_i=g^{ki},rk_i=MSK/k_i)$

S3:用户u_i与转换密钥rk_i以$\{u_i,rk_i\}$的形式保存在区块链中。

6.根据权利要求3所述的采用基于区块链的空间众包系统进行隐私保护的众包方法,其特征在于,所述步骤2的过程如下:

步骤2.1:任务请求者发布任务T_i,任务T_i包括任务的详细信息M_i,相关的任务关键词$W_i=\{w_1,w_2,...,w_i\}$以及任务位置坐标$R_i(x_i,y_i)$;

步骤2.2:采用AES高级加密方法生成对称密钥K_c,并用对称密钥K_c加密任务信息M_i得到密文C_i:$C_i=AesEnc(K_c,M_i)$;

步骤2.3:任务请求者采用RSA加密方法,使用自己的公钥加密对称密钥K_c得到密文C_{Pki}:$C_{PKi}=Enc(PK_r,K_c)$;

步骤2.4:将任务关键词进行哈希,将哈希值中的所有数字组成的字符串使用单独密钥qk_r加密,得到W_i':$W_i'=Enc(qk_r,W_i)$;

步骤2.5:采用线段树进行任务位置坐标的转换,并用单独密钥加密转换后的任务位置坐标R_i得到R_i',$R_i'=Enc(qk_r,R_i)$,$R_{rx}=\{l_{rx}\}\rightarrow R'_{rx}=\{l'_{rx}\}$,$R_{ry}=\{l_{ryl}\}\rightarrow R'_{ry}=\{l'_{ry}\}$;

其中,R_{rx}和l_{rx}均表示任务的经度,R'_{rx}和l'_{rx}均表示任务的经度加密后的密文,R_{ry}和l_{ry}均表示任务的纬度,R'_{ry}和l'_{ry}均表示任务的纬度加密后的密文;

步骤2.6:将生成的$T_i'=\{C_i,C_{PKi},W_i',R'_{rx},R'_{ry}\}$上传给代理$b_i$。

7.根据权利要求3所述的采用基于区块链的空间众包系统进行隐私保护的众包方法,其特征在于,所述步骤4的过程如下:

步骤4.1:工人在提交构造的搜索陷门时,先采用线段树进行位置坐标范围的转换:$(x1,x2)\rightarrow R_{wx}=\{l_{wx1},l_{wx2},...,l_{wxn}\}$,$(y1,y2)\rightarrow R_{wy}=\{l_{wy1},l_{wy2},...,l_{wyn}\}$;

其中,(x1,x2)为工人可以接受的任务的最大经度范围,(y1,y2)为工人可以接受的最大纬度范围,l_{wx}为其中的每一个经度转换后的路径的明文,l_{wy}为其中的每一个纬度转换后的路径的明文,R_{wx}为转换后的经度路径的明文的集合,R_{wy}为转换后的纬度路径明文集合;

步骤4.2:将兴趣关键字进行哈希,将哈希值中的所有数字组成的字符串使用自己的单

独密钥qk_w对其进行加密，形成搜索陷门$Td_1=Enc(qk_w,WW_w)=WW'_w$；

其中，WW_w为兴趣关键字，WW'_w为加密后的兴趣关键字；

步骤4.3：将位置进行哈希得到$Hwx=Hash(l_{wxi})$和$Hwy=Hash(l_{wyi})$用自己的单独密钥qk_w加密工人接受的任务范围，$R_{wx}=\{l_{wx1},l_{wx2},\ldots,l_{wxn}\}->R'_{wx}=\{l'_{wx1},l'_{wx2},\ldots,l'_{wxn}\}$，$R_{wy}=\{l_{wy1},l_{wy2},\ldots,l_{wyn}\}->R'_{wy}=\{l'_{wy1},l'_{wy2},\ldots,l'_{wyn}\}$，并形成搜索陷门$Td_2$：$Td_2=Enc(qk_w,R_{wx},R_{wy})=(R'_{wx},R'_{wy})=\{(g^{kw})^{lwx},(g^{kw})^{lwy}\}$；

其中，l_{wxi}为工人可以接受的每一个经度坐标路径的明文，l_{wyi}为工人可以接受的每一个纬度坐标路径的明文，R_{wx}为工人可以接受的经度坐标路径的明文集合，R'_{wx}为工人可以接受的任务经度坐标路径的密文集合，R_{wy}为工人可以接受的纬度坐标路径的明文集合，R'_{wy}工人可以接受的纬度坐标路径的密文集合，g^{kw}为工人的单独密钥，用来加密明文信息的；

步骤4.4：工人将生成的两个搜索陷门Td_1和Td_2上传到代理。

8.根据权利要求3所述的采用基于区块链的空间众包系统进行隐私保护的众包方法，其特征在于，所述步骤5的过程如下：

步骤5.1：代理对任务位置坐标密文进行重加密：

$((g^{kr})^{lrx})^{rk}=((g^{kr})^{lrx})^{MSK/k}=g^{lrx*MSK}$，$((g^{kr})^{lry})^{rkr}=((g^{kr})^{lry})^{MSK/k}=g^{lry*MSK}$

其中，g^{kr}为任务请求者的单独密钥，rk_r为任务请求者的单独密钥的转换密钥，kr为用于生成转换密钥的；

步骤5.2：代理对工人接受任务范围的坐标进行重加密：

$((g^{kw})^{lwx})^{rkw}=((g^{kw})^{lwx})^{MSK/kw}=g^{lwx*MSK}$，$((g^{kw})^{lwy})^{rkw}=((g^{kw})^{lwy})^{MSK/kw}=g^{lwy*MSK}$

其中，g^{kw}为工人的单独密钥，rk_w为工人的的单独密钥的转换密钥，kw为用于生成转换密钥的；

步骤5.3：调用匹配的智能合约，根据兴趣进行匹配：任务请求者的任务描述关键词中有与搜索陷门Td_1相匹配的，即：$W_i'=Td_1$；

步骤5.4：调用匹配的智能合约，根据位置匹配：工人的位置范围的密文集合中的$(R'_{rx},R'_{ry})\in(R'_{wx},R'_{wy})$即：

存在工人提交的坐标范围内一个点与点(R'_{rx},R'_{ry})重合：

任务请求者：$((g^{kw})^{lwx})^{rkw}=((g^{kw})^{lwx})^{MSK/kw}=g^{lwx*MSK}$，$((g^{kw})^{lwy})^{rkw}=((g^{kw})^{lwy})^{MSK/kw}=g^{lwy*MSK}$

工人：$((g^{kw})^{lwx})^{rkw}=((g^{kw})^{lwx})^{MSK/kw}=g^{lwx*MSK}$，$((g^{kw})^{lwy})^{rkw}=((g^{kw})^{lwy})^{MSK/kw}=g^{lwy*MSK}$

即：当且仅当存在一个点使$l_{rx}=l_{wx}$以及$l_{ry}=l_{wy}$时：

$g^{lrx*MSK}=g^{lwx*MSK}$，

$g^{lry*MSK}=g^{lwy*MSK}$，

判断当密文相等时，即在工人可接受的范围内包含该点，则该任务可以被分配给该工人；否则该任务不能分配给该工人。

9.根据权利要求3所述的采用基于区块链的空间众包系统进行隐私保护的众包方法，其特征在于，所述步骤6的过程如下：

步骤6.1：代理针对每个任务查看用户是否有查看该任务的权限，如果没有则，代理需要将工人的公钥发送给任务请求者，任务请求者使用工人的公钥和自己的私钥生成解密的

转换密钥ARK:$ARK=AEnc(PK_w,SK_r)$,并且发送给代理;

其中,PK_w为工人的公钥,SK_r为任务请求者的私钥;

步骤6.2:代理接收到转换密钥ARK,通过智能合约将其添加到任务请求者的授权列表中对授权列表进行更新;同样,任务请求者想要撤销某个工人的权限,通过代理调用智能合约将工人的授权的重加密转换密钥从自己的授权列表中删除;

步骤6.3:代理通过重加密转换密钥,将密文C_{PKi}转换为工人私钥可以解密的密文C'_{PKi}:$C'_{PKi}=ReEnc(ARK,C_{PKi})$,并将所有匹配的任务的密文进行转换并发送给工人。

10.根据权利要求3所述的采用基于区块链的空间众包系统进行隐私保护的众包方法,其特征在于,所述步骤7的过程如下:

步骤7.1:工人使用自己的私钥解密C_{PKi}得到K_c:$K_c=Des(SK_w,C_{PKi})$;

其中,K_c为加密任务信息的AES密钥,SK_w为工人的私钥,C_{PKi}为AES密钥的密文;

步骤7.2:使用得到的K_c解密T'_i得到任务信息明文T_i:$T_i=AESDes(K_c,T'_i)$。

一种基于区块链的空间众包系统及方法

技术领域

[0001] 本发明涉及任务匹配技术领域，尤其涉及一种基于区块链的空间众包系统及方法。

背景技术

[0002] 随着互联网的普及和发展，众包越来越受到人们的广泛关注。众包是指本应该由公司或机构的工人履行的职责，以及公开招募的方式将其外包给一个未知的人群的行为。空间众包需要工人到指定的地点完成指定的任务，在很多领域都有应用。

[0003] 在现在的众包平台(例如猪八戒等)中，基本上都是基于中心化的，而且不能保证第三方的可靠性，请求者和工人以及任务的信息可能存在泄露的风险，而且任务信息都是明文发布，请求者在系统中发布自己的任务，工人查看任务信息。如果存在恶意竞争的用户，可以根据任务的信息推断出任务的请求者，可能对任务请求者不利。而且根据任务的位置信息可以预测接受任务的工人的未来的位置，也会对造成工人位置信息的暴露。

[0004] 在IEEE Access第8卷的155819-155831页的论文“A Secure and Efficient Task Matching Scheme for Spatial Crowdsourcing”中提出的系统，通过密文实现了用户提交信息保护，对位置信息进行加密，在密文条件下进行任务匹配，但是未考虑到工人的兴趣问题，仅仅只是考虑了推荐工人在可接受距离的范围内的全部任务，需要工人在对任务兴趣进行二次筛选，用户体验降低。并且平台是中心化的，不可避免地单节点故障问题，由于存在第三方，无法保证代理的操作的透明性，则不可避免的存在用户隐私泄露的风险。

[0005] 在这个信息时代，人们对于自己的隐私格外重视，所以亟需一种既能实现请求者和工人任务在密文条件下进行匹配，保护用户隐私，并且监督众包平台的行为的方法。

发明内容

[0006] 针对上述现有技术的不足，本发明提供一种基于区块链的空间众包系统及方法。

[0007] 为解决上述技术问题，本发明所采取的技术方案是：一种基于区块链的空间众包系统，包括用户、密钥管理机构、代理、区块链网络和智能合约；

[0008] 所述密钥管理机构接收用户的注册申请，给用户发送个人公私钥以及单独密钥；并生成转换密钥，以{用户，转换密钥}的形式发送给代理进行管理；

[0009] 所述用户分为任务请求者和工人两种身份，所有用户能够在两种身份中切换角色；所述用户使用个人公私钥以及单独密钥给代理，由代理调用智能合约进行匹配；

[0010] 所述任务请求者使用自己的公私钥中的公钥加密任务信息，使用单独密钥加密任务坐标以及任务的关键词；

[0011] 所述工人使用自己的私钥解密经过代理重加密后的匹配到的任务密文得到任务信息，使用单独密钥加密自己的兴趣关键词以及接受的任务范围生成陷门，用来进行任务匹配；

[0012] 所述代理负责用户与区块链网络的交互，并提供相关的计算匹配服务；

[0013] 所述智能合约通过代理的调用情况，实现更新索引、代理重加密、任务匹配和维护授权列表的功能。

[0014] 进一步的，所述任务请求者根据需要授权工人访问自己的任务信息。

[0015] 另一方面，本发明还提供一种采用上述基于区块链的空间众包系统进行隐私保护的众包方法，包括如下步骤：

[0016] 步骤1：用户向密钥管理机构进行注册，由密钥管理机构为任务请求者和工人生成个人公私钥PK和SK、单独密钥qk以及转换密钥rk；

[0017] 所述个人公私钥中的公钥PK为公开状态，私钥SK为用户私有状态，不可公开；任务请求者的个人公私钥对记为(PK_r,SK_r)，工人的个人公私钥对记为(PK_w,SK_w)；

[0018] 所述公钥PK的生成过程为：

[0019] S1、用伪随机数生成器生成两个素数p和q，并将这两个素数相乘得到N：$N=p*q$；

[0020] S2、求解p-1和q-1的最小公倍数L：$L=lcm(p-1,q-1)$；

[0021] S3、在(1,L)范围内通过伪随机数生成E，判断$gcd(E,L)=1$是否成立，若成立则将得到的E和N作为公钥(E,N)，设为PK；

[0022] 所述私钥SK的生成过程为：在(1,L)范围内取D，同时使D满足$E*D \bmod L=1$的条件，将得到的D和N作为私钥(D,N)，设为SK。

[0023] 进一步的，所述任务请求者使用单独密钥qk_r加密任务位置坐标以及任务的关键词；所述工人使用单独密钥qk_w加密自己的兴趣关键词以及接受的任务范围生成搜索陷门，用来进行任务匹配；所述转换密钥rk由密钥管理机构以{用户，转换密钥}的形式发送给代理进行管理，用于任务匹配时进行重加密；所述任务请求者和工人对应的转换密钥分别为rk_r和rk_w；

[0024] 所述单独密钥qk和转换密钥rk的生成过程为：

[0025] S1：密钥管理机构生成随机数大质数g，生成一个公共哈希函数H，以及bigInteger类型的主密钥MSK：$(1\lambda)\rightarrow(g,H,MSK)$；

[0026] S2：对于一个用户u_i，密钥管理机构首先选择一个随机值k_i并且计算g^{ki}作为用户u_i的单独密钥qk_i，计算$rk_i=MSK/k_i$作为用户u_i的转换密钥rk_i：$(MSK,u_i)\rightarrow(qk_i=g^{ki},rk_i=MSK/k_i)$

[0027] S3：用户u_i与转换密钥rk_i以$\{u_i,rk_i\}$的形式保存在区块链中。

[0028] 步骤2：由任务请求者发布任务，同时使用任务请求者的公钥PKr加密任务信息，单独密钥qk_r加密任务位置坐标以及任务的关键词，过程如下：

[0029] 步骤2.1：任务请求者发布任务T_i，任务T_i包括任务的详细信息M_i，相关的任务关键词$W_i=\{w_1,w_2,...,w_i\}$以及任务位置坐标$R_i(x_i,y_i)$；

[0030] 步骤2.2：采用AES高级加密方法生成对称密钥K_c，并用对称密钥K_c加密任务信息M_i得到密文C_i：$C_i=AesEnc(K_c,M_i)$；

[0031] 步骤2.3：任务请求者采用RSA加密方法，使用自己的公钥加密对称密钥K_c得到密文C_{Pki}：$C_{PKi}=Enc(PK_r,K_c)$；

[0032] 步骤2.4：将任务关键词进行哈希，将哈希值中的所有数字组成的字符串使用单独密钥qk_r加密，得到W_i'：$W_i'=Enc(qk_r,W_i)$；

[0033] 步骤2.5：采用线段树进行任务位置坐标的转换，并用单独密钥加密转换后的任务

位置坐标R_i得到R_i'，$R_i'=Enc(qk_r,R_i)$，$R_{rx}=\{l_{rx}\}->R'_{rx}=\{l'_{rx}\}$，$R_{ry}=\{l_{ry1}\}->R'_{ry}=\{l'_{ry}\}$；

[0034] 其中，R_{rx}和l_{rx}均表示任务的经度，R'_{rx}和l'_{rx}均表示任务的经度加密后的密文，R_{ry}和l_{ry}均表示任务的纬度，R'_{ry}和l'_{ry}均表示任务的纬度加密后的密文；

[0035] 步骤2.6：将生成的$T_i'=\{C_i,C_{PKi},W_i',R'_{rx},R'_{ry}\}$上传给代理$b_i$。

[0036] 步骤3：代理收到任务请求者发送的任务相关的密文信息，为其生成相应的任务号t_i，将任务号以及对应的加密任务的关键词和任务位置坐标创建为任务索引上传到区块链网络；

[0037] 步骤4：工人使用自己的单独密钥加密自己的兴趣关键词以及接受的任务范围生成两个搜索陷门，并且上传到代理，过程如下：

[0038] 步骤4.1：工人在提交构造的搜索陷门时，先采用线段树进行位置坐标范围的转换：$(x1,x2)->R_{wx}=\{l_{wx1},l_{wx2},...,l_{wxn}\}$，$(y1,y2)->R_{wy}=\{l_{wy1},l_{wy2},...,l_{wyn}\}$；

[0039] 其中，(x1,x2)为工人可以接受的任务的最大经度范围，(y1,y2)为工人可以接受的最大纬度范围，l_{wx}为其中的每一个经度转换后的路径的明文，l_{wy}为其中的每一个纬度转换后的路径的明文，R_{wx}为转换后的经度路径的明文的集合，R_{wy}为转换后的纬度路径明文集合；

[0040] 步骤4.2：将兴趣关键字进行哈希，将哈希值中的所有数字组成的字符串使用自己的单独密钥qk_w对其进行加密，形成搜索陷门$Td_1=Enc(qk_w,WW_w)=WW'_w$；

[0041] 其中，WW_w为兴趣关键字，WW'_w为加密后的兴趣关键字；

[0042] 步骤4.3：将位置进行哈希得到$Hwx=Hash(l_{wxi})$和$Hwy=Hash(l_{wyi})$用自己的单独密钥qk_w加密工人接受的任务范围，$R_{wx}=\{l_{wx1},l_{wx2},...,l_{wxn}\}->R'_{wx}=\{l'_{wx1},l'_{wx2},...,l'_{wxn}\}$，$R_{wy}=\{l_{wy1},l_{wy2},...,l_{wyn}\}->R'_{wy}=\{l'_{wy1},l'_{wy2},...,l'_{wyn}\}$，并形成搜索陷门$Td_2$：$Td_2=Enc(qk_w,R_{wx},R_{wy})=(R'_{wx},R'_{wy})=\{(g^{kw})^{lwx},(g^{kw})^{lwy}\}$；

[0043] 其中，l_{wxi}为工人可以接受的每一个经度坐标路径的明文，l_{wyi}为工人可以接受的每一个纬度坐标路径的明文，R_{wx}为工人可以接受的经度坐标路径的明文集合，R'_{wx}为工人可以接受的任务经度坐标路径的密文集合，R_{wy}为工人可以接受的纬度坐标路径的明文集合，R'_{wy}工人可以接受的纬度坐标路径的密文集合，g^{kw}为工人的单独密钥，用来加密明文信息的；

[0044] 步骤4.4：工人将生成的两个搜索陷门Td_1和Td_2上传到代理。

[0045] 步骤5：代理先分别对任务位置坐标密文和工人接受任务范围的坐标进行重加密，然后代理调用匹配的智能合约将陷门与任务索引中的任务的关键词和任务位置坐标的密文进行匹配，将得到的结果返回给代理，过程如下：

[0046] 步骤5.1：代理对任务位置坐标密文进行重加密：

[0047] $((g^{kr})^{lrx})^{rk}=((g^{kr})^{lrx})^{MSK/k}=g^{lrx*MSK}$，$((g^{kr})^{lry})^{rkr}=((g^{kr})^{lry})^{MSK/k}=g^{lry*MSK}$

[0048] 其中，g^{kr}为任务请求者的单独密钥，rk_r为任务请求者的单独密钥的转换密钥，kr为用于生成转换密钥的；

[0049] 步骤5.2：代理对工人接受任务范围的坐标进行重加密：

[0050] $((g^{kw})^{lwx})^{rkw}=((g^{kw})^{lwx})^{MSK/kw}=g^{lwx*MSK}$，$((g^{kw})^{lwy})^{rkw}=((g^{kw})^{lwy})^{MSK/kw}=g^{lwy*MSK}$

[0051] 其中，g^{kw}为工人的单独密钥，rk_w为工人的的单独密钥的转换密钥，kw为用于生成

转换密钥的；

[0052] 步骤5.3：调用匹配的智能合约，根据兴趣进行匹配：任务请求者的任务描述关键词中有与搜索陷门Td_1相匹配的，即：$W_i' = Td_1$；

[0053] 步骤5.4：调用匹配的智能合约，根据位置匹配：工人的位置范围的密文集合中的$(R'_{rx}, R'_{ry}) \in (R'_{wx}, R'_{wy})$即：

[0054] 存在工人提交的坐标范围内一个点与点(R'_{rx}, R'_{ry})重合：

[0055] 任务请求者：$((g^{kw})^{lwx})^{rkw} = ((g^{kw})^{lwx})^{MSK/kw} = g^{lwx*MSK}$，$((g^{kw})^{lwy})^{rkw} = ((g^{kw})^{lwy})^{MSK/kw} = g^{lwy*MSK}$

[0056] 工人：$((g^{kw})^{lwx})^{rkw} = ((g^{kw})^{lwx})^{MSK/kw} = g^{lwx*MSK}$，$((g^{kw})^{lwy})^{rkw} = ((g^{kw})^{lwy})^{MSK/kw} = g^{lwy*MSK}$

[0057] 即：当且仅当存在一个点使$l_{rx} = l_{wx}$以及$l_{ry} = l_{wy}$时：

[0058] $g^{lrx*MSK} = d^{lwx*MSK}$，

[0059] $g^{lry*MSK} = g^{lwy*MSK}$，

[0060] 判断当密文相等时，即在工人可接受的范围内包含该点，则该任务可以被分配给该工人；否则该任务不能分配给该工人。

[0061] 步骤6：代理根据匹配到的任务，查询授权列表，查看工人是否在该任务请求者的授权列表中，如果不在，则向任务请求者申请，然后更新任务请求者的授权列表；并通过重加密转换密钥将所有匹配的任务的密文进行转换，将最终得到的转换后的任务密文发送给工人，过程如下：

[0062] 步骤6.1：代理针对每个任务查看用户是否有查看该任务的权限，如果没有则，代理需要将工人的公钥发送给任务请求者，任务请求者使用工人的公钥和自己的私钥生成解密的转换密钥ARK：$ARK = AEnc(PK_w, SK_r)$，并且发送给代理；

[0063] 其中，PK_w为工人的公钥，SK_r为任务请求者的私钥；

[0064] 步骤6.2：代理接收到转换密钥ARK，通过智能合约将其添加到任务请求者的授权列表中对授权列表进行更新；同样，任务请求者想要撤销某个工人的权限，通过代理调用智能合约将工人的授权的重加密转换密钥从自己的授权列表中删除；

[0065] 步骤6.3：代理通过重加密转换密钥，将密文C_{PKi}转换为工人私钥可以解密的密文C'_{PKi}：$C'_{PKi} = ReEnc(ARK, C_{PKi})$，并将所有匹配的任务的密文进行转换并发送给工人。

[0066] 步骤7：工人得到所有任务的密文后，进行解密操作得到任务信息明文，过程如下：

[0067] 步骤7.1：工人使用自己的私钥解密C_{PKi}得到K_c：$K_c = Des(SK_w, C_{PKi})$；

[0068] 其中，K_c为加密任务信息的AES密钥，SK_w为工人的私钥，C_{PKi}为AES密钥的密文；

[0069] 步骤7.2：使用得到的K_c解密T'_i得到任务信息明文T_i：$T_i = AESDes(K_c, T'_i)$。

[0070] 采用上述技术方案所产生的有益效果在于：

[0071] 1、本发明提供的系统和方法使用可搜索加密技术，无论是任务请求者还是工人提交的信息都是加密后的密文，因此代理以及其他人无法得到相关的明文信息，并且在任务匹配过程中，根据工人的兴趣和工人可接受的任务的距离同时匹配，只有满足了这两个条件才将任务加入到匹配列表，提高了任务匹配的精确度，能够极大的满足工人的需求，而且保护了用户的隐私。

[0072] 2、本发明通过代理重加密技术实现对请求者密文的转换以及相关的授权，如果请

求者允许某用户可以查看自己的发布任务信息，那么他可以使用自己的私钥以及工人的公钥为工人生成一个转换密钥，并将其发送给代理，代理通过该转换密钥可以将请求者加密的任务密文转换为工人私钥可以解密的密文，任务请求者可以通过该授权密钥的删除与上传控制工人对自己提交的任务的访问权限。

[0073] 3、本发明使用了区块链技术，避免了单点故障，以及通过智能合约，代理上传任务索引，进行任务匹配，授权和撤销工人权限以及密文转换等操作都会被记录在区块链网络中，所有区块链上的节点都存有备份可以进行监督，保证了信息的透明性。

附图说明

[0074] 图1为本发明实施例中提供的基于区块链的空间众包系统的结构示意图；

[0075] 图2为本发明实施例中提供的采用基于区块链的空间众包系统进行隐私保护的众包方法的流程图。

具体实施方式

[0076] 下面结合附图和实施例，对本发明的具体实施方式作进一步详细描述。以下实施例用于说明本发明，但不用来限制本发明的范围。

[0077] 如图1所示，本实施例中基于区块链的空间众包系统如下所述：

[0078] 系统包括用户、密钥管理机构、代理、区块链网络和智能合约；

[0079] 所述密钥管理机构接收用户的注册申请，给用户发送个人公私钥以及单独密钥；并生成转换密钥，以{用户，转换密钥}的形式发送给代理进行管理；

[0080] 所述用户分为任务请求者和工人两种身份，所有用户能够在两种身份中切换角色；所述用户使用个人公私钥以及单独密钥给代理，由代理调用智能合约进行匹配；

[0081] 所述任务请求者使用自己的公私钥中的公钥加密任务信息，使用单独密钥加密任务坐标以及任务的关键词；

[0082] 所述工人使用自己的私钥解密经过代理重加密后的匹配到的任务密文得到任务信息，使用单独密钥加密自己的兴趣关键词以及接受的任务范围生成陷门，用来进行任务匹配；

[0083] 所述代理负责用户与区块链网络的交互，并提供相关的计算匹配服务；

[0084] 所述智能合约通过代理的调用情况，实现更新索引、代理重加密、任务匹配和维护授权列表的功能。

[0085] 进一步的，所述任务请求者根据需要授权工人访问自己的任务信息。

[0086] 本实施例中还提供一种采用上述基于区块链的空间众包系统进行隐私保护的众包方法，其流程如图2所示，包括如下步骤：

[0087] 步骤1：用户向密钥管理机构进行注册，由密钥管理机构为任务请求者和工人生成个人公私钥PK和SK、单独密钥qk以及转换密钥rk；

[0088] 所述个人公私钥中的公钥PK为公开状态，私钥SK为用户私有状态，不可公开；任务请求者的个人公私钥对记为(PK_r,SK_r)，工人的个人公私钥对记为(PK_w,SK_w)；

[0089] 所述公钥PK的生成过程为：

[0090] S1、用伪随机数生成器生成两个素数p和q，并将这两个素数相乘得到N：$N=p*q$；

[0091] S2、求解p-1和q-1的最小公倍数L:L＝lcm(p-1,q-1)；

[0092] S3、在(1,L)范围内通过伪随机数生成E,判断gcd(E,L)＝1是否成立,若成立则将得到的E和N作为公钥(E,N),设为PK；

[0093] 所述私钥SK的生成过程为:在(1,L)范围内取D,同时使D满足E*D mod L＝1的条件,将得到的D和N作为私钥(D,N),设为SK。

[0094] 进一步的,所述任务请求者使用单独密钥qk_r加密任务位置坐标以及任务的关键词;所述工人使用单独密钥qk_w加密自己的兴趣关键词以及接受的任务范围生成搜索陷门,用来进行任务匹配;所述转换密钥rk由密钥管理机构以{用户,转换密钥}的形式发送给代理进行管理,用于任务匹配时进行重加密;所述任务请求者和工人对应的转换密钥分别为rk_r和rk_w；

[0095] 所述单独密钥qk和转换密钥rk的生成过程为：

[0096] S1:密钥管理机构生成随机数大质数g,生成一个公共哈希函数H,以及bigInteger类型的主密钥MSK:(1λ)->(g,H,MSK)；

[0097] S2:对于一个用户u_i,密钥管理机构首先选择一个随机值k_i并且计算g^{ki}作为用户u_i的单独密钥qk_i,计算rk_i＝MSK/k_i作为用户u_i的转换密钥rk_i:(MSK,u_i)->($qk_i＝g^{ki}$,rk_i＝MSK/k_i)

[0098] S3:用户u_i与转换密钥rk_i以{u_i,rk_i}的形式保存在区块链中。

[0099] 步骤2:由任务请求者发布任务,同时使用任务请求者的公钥PKr加密任务信息,单独密钥qk_r加密任务位置坐标以及任务的关键词,过程如下：

[0100] 步骤2.1:任务请求者发布任务T_i,任务T_i包括任务的详细信息M_i,相关的任务关键词$W_i＝\{w_1,w_2,...,w_i\}$以及任务位置坐标$R_i(x_i,y_i)$；

[0101] 步骤2.2:采用AES高级加密方法生成对称密钥K_c,并用对称密钥K_c加密任务信息M_i得到密文C_i:$C_i＝AesEnc(K_c,M_i)$；

[0102] 步骤2.3:任务请求者采用RSA加密方法,使用自己的公钥加密对称密钥K_c得到密文C_{Pki}:$C_{PKi}＝Enc(PK_r,K_c)$；

[0103] 步骤2.4:将任务关键词进行哈希,将哈希值中的所有数字组成的字符串使用单独密钥qk_r加密,得到W_i':$W_i'＝Enc(qk_r,W_i)$；

[0104] 步骤2.5:采用线段树进行任务位置坐标的转换,并用单独密钥加密转换后的任务位置坐标R_i得到R_i',$R_i'＝Enc(qk_r,R_i)$,$R_{rx}＝\{l_{rx}\}->R'_{rx}＝\{l'_{rx}\}$,$R_{ry}＝\{l_{ryl}\}->R'_{ry}＝\{l'_{ry}\}$；

[0105] 其中,R_{rx}和l_{rx}均表示任务的经度,R'_{rx}和l'_{rx}均表示任务的经度加密后的密文,R_{ry}和l_{ry}均表示任务的纬度,R'_{ry}和l'_{ry}均表示任务的纬度加密后的密文；

[0106] 本实施例中,所述采用线段树进行任务位置坐标的转换,先将经纬度换分为不同的小区域,即转换为序号不同的树,再将具体经纬度转换为树上的叶节点的路径,从而将树的序号和叶结点的路径进行合并,同理,将工人的可接受的任务的范围进行相同的转换,转换为一个字符串集合。

[0107] 步骤2.6:将生成的$T_i'＝\{C_i,C_{PKi},W_i',R'_{rx},R'_{ry}\}$上传给代理$b_i$。

[0108] 步骤3:代理收到任务请求者发送的任务相关的密文信息,为其生成相应的任务号t_i,将任务号以及对应的加密任务的关键词和任务位置坐标创建为任务索引上传到区块链

网络；

[0109] 步骤4：工人使用自己的单独密钥加密自己的兴趣关键词以及接受的任务范围生成两个搜索陷门，并且上传到代理，过程如下：

[0110] 步骤4.1：工人在提交构造的搜索陷门时，先采用线段树进行位置坐标范围的转换：$(x1,x2)->R_{wx}=\{l_{wx1},l_{wx2},\ldots,l_{wxn}\}$，$(y1,y2)->R_{wy}=\{l_{wy1},l_{wy2},\ldots,l_{wyn}\}$；

[0111] 其中，(x1,x2)为工人可以接受的任务的最大经度范围，(y1,y2)为工人可以接受的最大纬度范围，l_{wx}为其中的每一个经度转换后的路径的明文，l_{wy}为其中的每一个纬度转换后的路径的明文，R_{wx}为转换后的经度路径的明文的集合，R_{wy}为转换后的纬度路径明文集合；

[0112] 步骤4.2：将兴趣关键字进行哈希，将哈希值中的所有数字组成的字符串使用自己的单独密钥qk_w对其进行加密，形成搜索陷门$Td_1=Enc(qk_w,WW_w)=WW'_w$；

[0113] 其中，WW_w为兴趣关键字，WW'_w为加密后的兴趣关键字；

[0114] 步骤4.3：将位置进行哈希得到$Hwx=Hash(l_{wxi})$和$Hwy=Hash(l_{wyi})$用自己的单独密钥qk_w加密工人接受的任务范围，$R_{wx}=\{l_{wx1},l_{wx2},\ldots,l_{wxn}\}->R'_{wx}=\{l'_{wx1},l'_{wx2},\ldots,l'_{wxn}\}$，$R_{wy}=\{l_{wy1},l_{wy2},\ldots,l_{wyn}\}->R'_{wy}=\{l'_{wy1},l'_{wy2},\ldots,l'_{wyn}\}$，并形成搜索陷门$Td_2$：$Td_2=Enc(qk_w,R_{wx},R_{wy})=(R'_{wx},R'_{wy})=\{(g^{kw})^{lwx},(g^{kw})^{lwy}\}$；

[0115] 其中，l_{wxi}为工人可以接受的每一个经度坐标路径的明文，l_{wyi}为工人可以接受的每一个纬度坐标路径的明文，R_{wx}为工人可以接受的经度坐标路径的明文集合，R'_{wx}为工人可以接受的任务经度坐标路径的密文集合，R_{wy}为工人可以接受的纬度坐标路径的明文集合，R'_{wy}工人可以接受的纬度坐标路径的密文集合，g^{kw}为工人的单独密钥，用来加密明文信息的；

[0116] 步骤4.4：工人将生成的两个搜索陷门Td_1和Td_2上传到代理。

[0117] 步骤5：代理先分别对任务位置坐标密文和工人接受任务范围的坐标进行重加密，然后代理调用匹配的智能合约将陷门与任务索引中的任务的关键词和任务位置坐标的密文进行匹配，将得到的结果返回给代理，过程如下：

[0118] 步骤5.1：代理对任务位置坐标密文进行重加密：

[0119] $((g^{kr})^{lrx})^{rk}=((g^{kr})^{lrx})^{MSK/k}=g^{lrx*MSK}$，$((g^{kr})^{lry})^{rkr}=((g^{kr})^{lry})^{MSK/k}=g^{lry*MSK}$

[0120] 其中，g^{kr}为任务请求者的单独密钥，rk_r为任务请求者的单独密钥的转换密钥，kr为用于生成转换密钥的；

[0121] 步骤5.2：代理对工人接受任务范围的坐标进行重加密：

[0122] $((g^{kw})^{lwx})^{rkw}=((g^{kw})^{lwx})^{MSK/kw}=g^{lwx*MSK}$，$((g^{kw})^{lwy})^{rkw}=((g^{kw})^{lwy})^{MSK/kw}=g^{lwy*MSK}$

[0123] 其中，g^{kw}为工人的单独密钥，rk_w为工人的的单独密钥的转换密钥，kw为用于生成转换密钥的；

[0124] 步骤5.3：调用匹配的智能合约，根据兴趣进行匹配：任务请求者的任务描述关键词中有与搜索陷门Td_1相匹配的，即：$W_i'=Td_1$；

[0125] 步骤5.4：调用匹配的智能合约，根据位置匹配：工人的位置范围的密文集合中的$(R'_{rx},R'_{ry})\in(R'_{wx},R'_{wy})$即：

[0126] 存在工人提交的坐标范围内一个点与点(R'_{rx},R'_{ry})重合：

[0127] 任务请求者：$((g^{kw})^{lwx})^{rkw}=((g^{kw})^{lwx})^{MSK/kw}=g^{lwx*MSK}$，$((g^{kw})^{lwy})^{rkw}=((g^{kw})^{lwy})^{MSK/kw}$

$=g^{lwy*MSK}$

[0128] 工人：$((g^{kw})^{lwx})^{rkw}=((g^{kw})^{lwx})^{MSK/kw}=g^{lwx*MSK}$，$((g^{kw})^{lwy})^{rkw}=((g^{kw})^{lwy})^{MSK/kw}=g^{lwy*MSK}$

[0129] 即：当且仅当存在一个点使$l_{rx}=l_{wx}$以及$l_{ry}=l_{wy}$时：

[0130] $g^{lrrx*MSK}=g^{lwx*MSK}$，

[0131] $g^{lry*MSK}=g^{lwy*MSK}$，

[0132] 判断当密文相等时，即在工人可接受的范围内包含该点，则该任务可以被分配给该工人；否则该任务不能分配给该工人。

[0133] 步骤6：代理根据匹配到的任务，查询授权列表，查看工人是否在该任务请求者的授权列表中，如果不在，则向任务请求者申请，然后更新任务请求者的授权列表；并通过重加密转换密钥将所有匹配的任务的密文进行转换，将最终得到的转换后的任务密文发送给工人，过程如下：

[0134] 步骤6.1：代理针对每个任务查看用户是否有查看该任务的权限，如果没有则，代理需要将工人的公钥发送给任务请求者，任务请求者使用工人的公钥和自己的私钥生成解密的转换密钥ARK：$ARK=AEnc(PK_w,SK_r)$，并且发送给代理；

[0135] 其中，PK_w为工人的公钥，SK_r为任务请求者的私钥；

[0136] 步骤6.2：代理接收到转换密钥ARK，通过智能合约将其添加到任务请求者的授权列表中对授权列表进行更新；同样，任务请求者想要撤销某个工人的权限，通过代理调用智能合约将工人的授权的重加密转换密钥从自己的授权列表中删除；

[0137] 步骤6.3：代理通过重加密转换密钥，将密文C_{PKi}转换为工人私钥可以解密的密文C'_{PKi}：$C'_{PKi}=ReEnc(ARK,C_{PKi})$，并将所有匹配的任务的密文进行转换并发送给工人。

[0138] 此外，如果任务请求者想要撤销某个工人的权限，可以通过代理，调用智能合约将工人的授权的重加密转换密钥从自己的授权列表中删除。

[0139] 步骤7：工人得到所有任务的密文后，进行解密操作得到任务信息明文，过程如下：

[0140] 步骤7.1：工人使用自己的私钥解密C_{PKi}得到K_c：$K_c=Des(SK_w,C_{PKi})$；

[0141] 其中，K_c为加密任务信息的AES密钥，SK_w为工人的私钥，C_{PKi}为AES密钥的密文；

[0142] 步骤7.2：使用得到的K_c解密T'_i得到任务信息明文T_i：$T_i=AESDes(K_c,T'_i)$。

[0143] 本实施例中，对众包系统中1000个工人和50000条任务的数据进行匹配，由于使用哈希散列表，时间复杂度为O(1)，方法的匹配过程花费的平均时间为3ms，在可接受的范围内。基本满足了空间众包中用户隐私保护需求，实现了对众包平台的监督，保证了平台信息透明，并且任务匹配的更符合工人的需求，同时匹配的时间在可接受的范围内，达到了应用的要求。

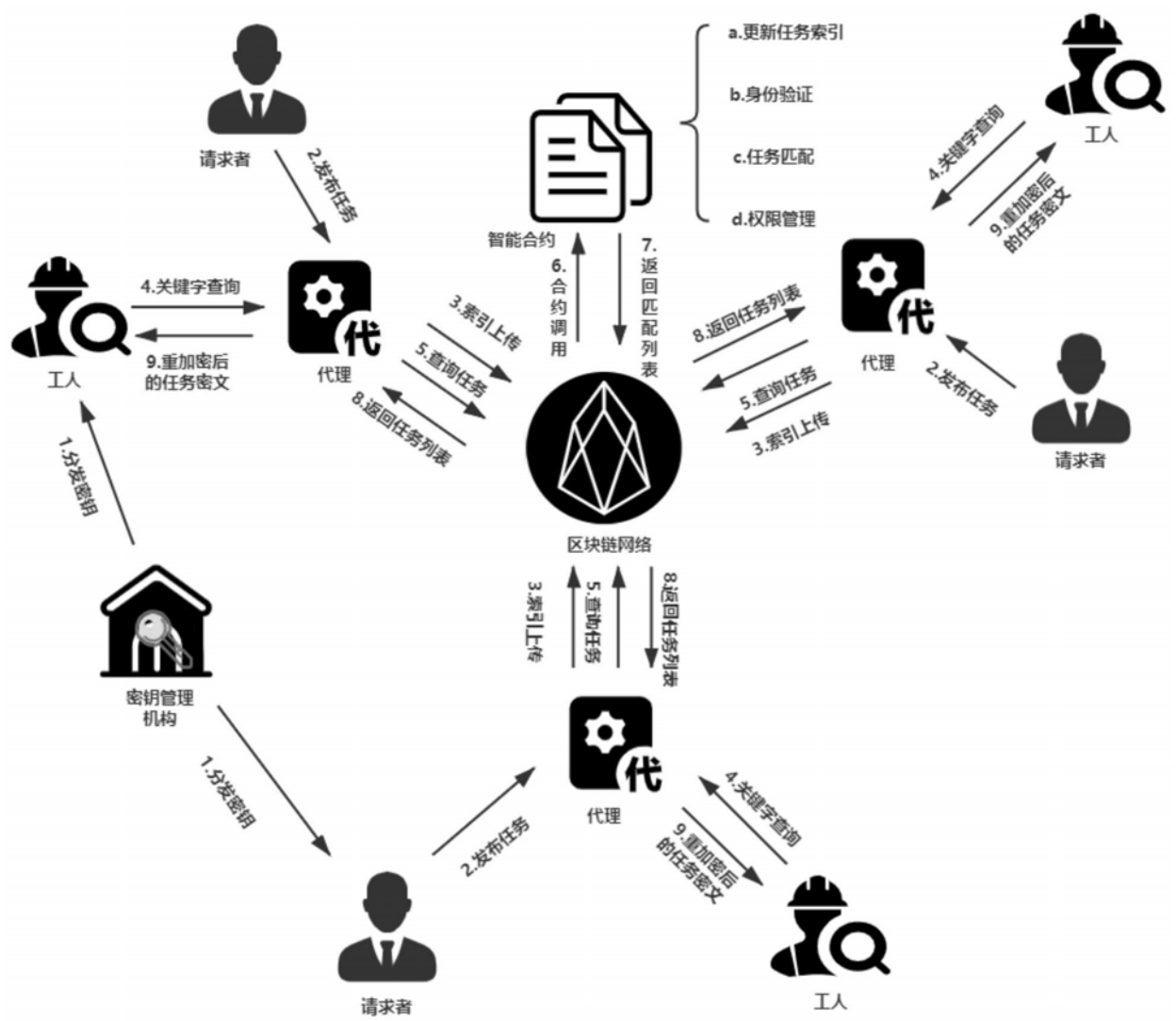

请求者
2.发布任务
智能合约
a.更新任务索引
b.身份验证
c.任务匹配
d.权限管理
工人
4.关键字查询
9.重加密后的任务密文
工人
4.关键字查询
9.重加密后的任务密文
代理
3.索引上传
5.查询任务
8.返回任务列表
6.合约调用
7.返回匹配列表
代理
8.返回任务列表
5.查询任务
3.索引上传
2.发布任务
请求者
1.分发密钥
区块链网络
3.索引上传
5.查询任务
8.返回任务列表
密钥管理机构
1.分发密钥
2.发布任务
代理
4.关键字查询
9.重加密后的任务密文
请求者
工人

图1


密钥管理机构向用户发布密钥
任务请求者发布任务，同时对任务进行加密
代理收到任务相关的密文信息，创建任务索引上传到区块链网络
工人通过密钥生成两个搜索陷门上传到代理
代理先进行重加密，然后调用匹配的智能合约将陷门与任务密文进行匹配，结果返回给代理
代理访问授权列表，通过重加密转换密钥将任务的密文进行转换，转换后的任务密文发送给工人
工人对任务密文进行解密，得到任务明文

图2