(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 110046521 A
(43)申请公布日 2019.07.23

(21)申请号 201910331651.1

(22)申请日 2019.04.24

(71)申请人 成都派沃特科技股份有限公司
地址 610000 四川省成都市高新区天华二路219号天府软件园C区12栋14层

(72)发明人 黄希 聂贻俊 刘翼 梁松 宋晓梅

(74)专利代理机构 北京天奇智新知识产权代理有限公司 11340
代理人 杨春

(51)Int.Cl.
G06F 21/62(2013.01)
G06F 21/60(2013.01)
G06Q 50/00(2012.01)
H04L 29/08(2006.01)

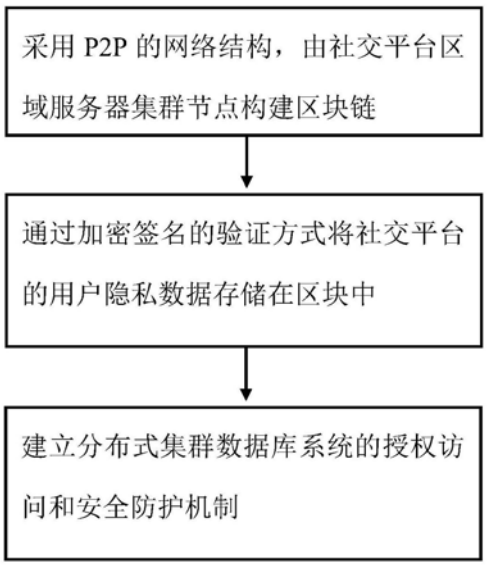
权利要求书1页 说明书9页 附图1页

(54)发明名称

去中心化隐私保护方法

(57)摘要

本发明提供了一种去中心化隐私保护方法，该方法包括：采用P2P的网络结构，由社交平台区域服务器集群节点构建区块链，通过加密签名的验证方式将社交平台的用户隐私数据存储在区块中，建立分布式集群数据库系统的授权访问和安全防护机制。本发明提出了一种去中心化隐私保护方法，实现了社交网络中用户隐私数据的去中心化存储和认证，认证过程在区块链中完成，利用区块链的不可篡改性确保用户身份的有效性，使用数据摘要代替用户个人信息明文，根据数据摘要为用户匹配信息，即使恶意攻击者截取用户信息也无法查看用户隐私信息明文，保护了用户的隐私。



CN 110046521 A

1.一种去中心化隐私保护方法,包括:

采用P2P的网络结构,由社交平台区域服务器集群节点构建区块链,通过加密签名的验证方式将社交平台的用户隐私数据存储在区块中,建立分布式集群数据库系统的授权访问和安全防护机制。

2.根据权利要求1所述的方法,其特征在于,所述用户隐私数据包含通信数据块信息、用户身份信息、个人属性信息和会话内容信息。

3.根据权利要求1所述的方法,其特征在于,所述通过加密签名的验证方式将社交平台的用户隐私数据存储在区块中,进一步包括:

使用私钥对用于加密用户隐私数据的对称密钥进行加密,并使用公钥对加密后的对称密钥信息解密;私钥所有者解密后,可以使用对称密钥,解密后获得用户信息;私钥对用户信息签名,公钥验证签名;通过公钥签名验证的信息确认为私钥所有者发出。

4.根据权利要求1所述的方法,其特征在于,所述方法还包括,将用户隐私信息明文通过伪随机映射生成密文,再将密文按照随机序列交由区块链上的区块进行加密存储,并将存储数据的区块号信息反馈至加密节点生成相应的权限,将该密文提交至区块链多个节点共同维护,只有许可证中具备相应权限的区块节点才拥有数据解密信息。

5.根据权利要求4所述的方法,其特征在于,所述将该密文提交至区块链多个节点共同维护,进一步包括:

将密文分为N个密文块,将密文块进行编号;将块头存储在集群管理节点中,将其余密文块的编号置乱后按区块链连接顺序发送给链上的集群节点;接收数据的节点根据本地的加密算法对接收到的数据再次加密,加密信息存储在该节点的许可证中;只有当某个节点中的许可证拥有该权限才可以获得索引信息,进而获取其余区块上的加密数据并对密文进行还原。

6.根据权利要求1所述的方法,其特征在于,所述方法还包括,区域服务器集群的每个节点进入P2P网络前,预设网络接入许可证,该许可证基于节点所属区域、节点类型、节点唯一标识、有效期信息而使用该区域私钥离线加密生成。

去中心化隐私保护方法

技术领域

[0001] 本发明涉及社交网络,特别涉及一种去中心化隐私保护方法。

背景技术

[0002] 近年来,微信、论坛、微博等社交网络发展迅猛,人们也通常会同时加入多个社交平台来享受互联网提供的便利与完整的服务。以两个社交平台为例,已经在其中一个平台中注册过的用户想要新加入另一个平台,则就会向原始平台发送请求询问该用户的基本信息,以便为其提供个性化服务。而传统的身份认证方法存在用户隐私泄露、伪造认证信息和平台对已认证行为的抵赖问题。更严重的是,社交网络平台对海量用户相关信息进行调查,用户提供系统以海量的明文信息,最后统一收集形成中心化的数据库。平台利用用户个人信息和会话信息进行数据挖掘,采集用户个人特征或爱好。例如Facebook公司,多次涉嫌侵犯用户隐私,2018年一家第三方公司获取了超过5000万Facebook用户的数据信息,通过算法建构用户画像并设计软件程序,进而预测和干涉选民的投票意向和行为。甚至有第三方平台利用海量用户信息,不断对用户进行推荐和骚扰,无法保证用户个人隐私安全。

发明内容

[0003] 为解决上述现有技术所存在的问题,本发明提出了一种去中心化隐私保护方法,包括:

[0004] 采用P2P的网络结构,由社交平台区域服务器集群节点构建区块链,通过加密签名的验证方式将社交平台的用户隐私数据存储在区块中,建立分布式集群数据库系统的授权访问和安全防护机制。

[0005] 优选地,所述用户隐私数据包含通信数据块信息、用户身份信息、个人属性信息和会话内容信息。

[0006] 优选地,所述通过加密签名的验证方式将社交平台的用户隐私数据存储在区块中,进一步包括:

[0007] 使用私钥对用于加密用户隐私数据的对称密钥进行加密,并使用公钥对加密后的对称密钥信息解密;私钥所有者解密后,可以使用对称密钥,解密后获得用户信息;私钥对用户信息签名,公钥验证签名;通过公钥签名验证的信息确认为私钥所有者发出。

[0008] 优选地,所述方法还包括,将用户隐私信息明文通过伪随机映射生成密文,再将密文按照随机序列交由区块链上的区块进行加密存储,并将存储数据的区块号信息反馈至加密节点生成相应的权限,将该密文提交至区块链多个节点共同维护,只有许可证中具备相应权限的区块节点才拥有数据解密信息。

[0009] 优选地,所述将该密文提交至区块链多个节点共同维护,进一步包括:

[0010] 将密文分为N个密文块,将密文块进行编号;将块头存储在集群管理节点中,将其余密文块的编号置乱后按区块链连接顺序发送给链上的集群节点;接收数据的节点根据本地的加密算法对接收到的数据再次加密,加密信息存储在该节点的许可证中;只有当某个

节点中的许可证拥有该权限才可以获得索引信息，进而获取其余区块上的加密数据并对密文进行还原。

[0011] 优选地，所述方法还包括，区域服务器集群的每个节点进入P2P网络前，预设网络接入许可证，该许可证基于节点所属区域、节点类型、节点唯一标识、有效期信息而使用该区域私钥离线加密生成。

[0012] 本发明相比现有技术，具有以下优点：

[0013] 本发明提出了一种去中心化隐私保护方法，实现了社交网络中用户隐私数据的去中心化存储和认证，认证过程在区块链中完成，利用区块链的不可篡改性确保用户身份的有效性，使用数据摘要代替用户个人信息明文，根据数据摘要为用户匹配信息，即使恶意攻击者截取用户信息也无法查看用户隐私信息明文，保护了用户的隐私。

附图说明

[0014] 图1是根据本发明实施例的去中心化隐私保护方法的流程图。

具体实施方式

[0015] 下文与图示本发明原理的附图一起提供对本发明一个或者多个实施例的详细描述。结合这样的实施例描述本发明，但是本发明不限于任何实施例。本发明的范围仅由权利要求书限定，并且本发明涵盖诸多替代、修改和等同物。在下文描述中阐述诸多具体细节以便提供对本发明的透彻理解。出于示例的目的而提供这些细节，并且无这些具体细节中的一些或者所有细节也可以根据权利要求书实现本发明。

[0016] 本发明的一方面提供了一种去中心化隐私保护方法。图1是根据本发明实施例的去中心化隐私保护方法流程图。

[0017] 本发明提出一种基于区块链的社交平台用户隐私保护体系，采用P2P的网络结构，以社交平台区域服务器集群节点构建区块链，并建立分布式集群数据库系统的授权访问和安全防护机制。各区域服务器集群节点将用户个人数据存储在区块链中，并通过加密签名的验证方式将单独的区块链成首尾相接的形式。社交平台区块链系统包含数据存储模块、密码模块、共识模块和智能合约模块。

[0018] 数据存储模块中，区块头存储结构包含版本号、时间戳、记录类型、类型数量、节点代码、节点标识、节点权限、算法计数器、Merkle根、前驱区块头；其中版本号记录了当前区块生成时所属的系统版本信息。时间戳记录当前区块的生成时间戳。记录类型记录了当前区块体中所包含的社交信息的类型，标识字符串每位代表一种类型，记录类型包括用户身份信息、个人属性信息、用户状态信息、社交会话信息以及社交网络中的其他信息。类型数量记录当前区块的区块体中所包含的社交信息记录的数量，按记录类型分别计数。节点代码记录当前区块的生成节点的HASH值，便于快速定位区块对应的生成节点。节点标识记录当前区块建立时，对应生成节点的等级信息。节点权限记录当前区块建立时，对应生成节点的权限信息，为不同共识算法提供可识别信息。算法计数器为共识算法提供数据支持，将共识算法所需的关键信息记录到区块中。Merkle根记录交易树的树根HASH值。当每次区块被打包的时候，该字段需要重新计算更新一次，Merkle根为该区块中所有被记录交易的根节点HASH值。前驱区块头为当前区块前一个区块的区块头的HASH值。

[0019] 其次，区块体包含通信数据块信息、用户身份信息、个人属性信息和会话内容信息的社交网络数据记录，并采用Merkle树结构来进行记录。采用对称加密算法对原始信息进行加密，通过HASH算法形成加密信息摘要，通过非对称加密算法进行签名，设计符合社交隐私信息保护特征的区块链Merkle树与布隆过滤器，从而构成防篡改、可追溯的可信数据链。

[0020] 社交网络数据记录按照时间顺序生成。且每次社交网络数据记录都有索引编号以供查询。其记录包括生成时间戳、HASH值、数据记录的索引编号以及关键信息等细节。每一个数据记录都对应一个Merkle节点值，而这个HASH值是Merkle树的一部分，因此每一个地址都不能重复写入或伪造。每个事件都有时间戳，成为一条长链的一部分，且无法在事后进行篡改。通过在区块链上设置权限限制，各集群节点通过协商，确定可以访问的通信内容，从而维持用户数据的隐私性。

[0021] 密码模块用于将区块数据进行加密。在加密过程中，使用私钥对加密用户信息的对称密钥进行加密，并使用公钥对加密后的对称密钥信息解密。私钥所有者解密后，可以使用对称密钥，解密后获得用户信息。私钥对用户信息签名，公钥验证签名。通过公钥签名验证的信息确认为私钥所有者发出。由于没有可信任的中心，传统方法由各节点自主保存私钥，为避免私钥丢失以使认证信息的永久失效，本发明的密码模块设置集中式的密钥中心，对所有节点密钥进行统一管理，所有节点在接入区块链前都需要在密钥中心中注册，分配相应的公钥和私钥，只有获取了集群节点的私钥才能够解密由公钥加密的信息，而通过密钥中心获取丢失的私钥，确保区块链上数据可以被真实还原。

[0022] 为实现将密文交由所有节点共同存储和维护，在进一步优选的实施例中，所述密码模块将明文通过伪随机映射生成密文，再将密文按照随机序列交由区块链上的区块进行加密存储，并将存储数据的区块号信息反馈至加密节点生成相应的权限。此后密文由区块链共同维护，只有许可证中具备相应权限的区块节点才拥有数据解密信息。

[0023] 首先，使用两个伪随机映射，设置μ_0和μ_1分别为两个伪随机映射的密钥分支参数，x_0和x_1分别为两个密钥序列初始值，按照μ_0，x_0，μ_1，x_1分别产生$m\times n$个随机数，其中μ_0和μ_1分别为两个伪随机映射的分支参数，x_0和x_1分别为两个伪随机映射的序列初始值，生成序列$L_1(k)$、$L_2(k)$，并合成$m\times n$大小的随机矩阵$Z_1(i,j)_{m\times n}$，$Z_2(i,j)_{m\times n}$；其中，$i\in[1,m]$，$j\in[1,n]$；

[0024] 根据公式a_i和b_i分别抽取$L_1(k)$、$L_2(k)$相应位，并作为下一次抽取的初始位；

[0025] $$a_i=\lfloor(\mathrm{mod}(10^{(b_{i-1}+1)}\times L_1(k),10))\rfloor$$

[0026] $$b_i=\lfloor(\mathrm{mod}(10^{(a_{i-1}+1)}\times L_2(k),10))\rfloor$$

[0027] 其中，初始位置b_0根据明文数据的信息熵确定，信息熵值用h表示。

[0028] $$b_0=\lfloor(\mathrm{mod}(10^3\times h,10))\rfloor$$

[0029] 迭代计算a_i和b_i，使$k=1,2,\cdots,m\times n$，直到$L_1(k)$、$L_2(k)$遍历序列得到a_k和b_k；

[0030] 由序列a_k和b_k合成$m\times n$的中间矩阵$F(i,j)$，根据以下公式转换成二进制随机矩阵$Z_3(i,j)_{m\times n}$：

[0031] $$Z_3(i,j)=\begin{cases}1 & F(i,j)\geq 5\\ 0 & F(i,j)<5\end{cases}$$

[0032] 将$Z_3(i,j)_{m\times n}$进行标准互补配对编码，得到对应的编码矩阵$Z_4(i,j)_{m\times n}$；

[0033] 将原始明文数据转换成二进制的$K(i,j)_{m\times n}$矩阵，具体地，首先根据互补配对编码规则进行编码，然后选取置换规则生成乱序的编码$K_{disorder}(i,j)_{m\times n}$；

[0034] 计算矩阵$Z_4(i,j)_{m\times n}+K_{disorder}(i,j)_{m\times n}=H_{disorder}(i,j)_{m\times n}$，并将根据预先选取的所述置换规则进行相应解码，得到$K_1(i,j)_{m\times n}$；

[0035] 选取随机矩阵$Z_1(i,j)_{m\times n}$，$Z_2(i,j)_{m\times n}$，根据下列公式对矩阵$K_1(i,j)_{m\times n}$进行置乱：

[0036] $temp=K_1(i,j)$；

[0037] $K_1(i,j)=K(X(i,j),Y(i,j))$；

[0038] $K(X(i,j),Y(i,j))=temp$；

[0039] 其中：

[0040] $$X(i,\ j)=\mathrm{mod}\lfloor(a_1\times Z_1(i,j),\ x)\rfloor,$$

[0041] $$Y(i,\ j)=\mathrm{mod}\lfloor(b_1\times Z_2(i,j),\ y)\rfloor,\ y);$$

[0042] x和y分别为明文矩阵的行列值；

[0043] 重复上述置乱步骤，直到将矩阵$K_1(i,j)_{m\times n}$全部遍历w次，遍历次数w可根据加密强度进行选择，得到置乱后的加密矩阵并生成相应的信息数据，完成加密。

[0044] 将密文分为N个密文块，将密文块进行编号(0,1,2,3,…,N-1)。将块头存储在集群管理节点中，将其余密文块的编号置乱后按区块链连接顺序发送给链上的集群节点。接收数据的节点根据本地的加密算法对接收到的数据再次加密，加密信息存储在该节点的许可证中。由于密文交由区块链节点节点共同存储、共同维护，因此增加了破译难度。只有当某个节点中的许可证拥有该权限才可以获得索引信息，进而获取其余区块上的加密数据并对密文进行还原，保障了信息的私密性。

[0045] 在社交网络集群节点的存储架构上，首先在多个区域服务器集群节点里选择多个管理节点，这些管理节点与普通节点组成一个P2P网络簇，管理节点保存当前区域其余普通节点全部路由信息以及全网其他节点的部分路由信息，管理节点之间同步路由信息和发现算法。

[0046] 每个节点启动时，首先计算自己的计算能力值，然后在局域网内通过广播寻找管理节点，即返回给这个节点当前网络内最高计算能力值前n名列表及节点地址，节点根据列表比较自己计算出的计算能力值，如果自己属于普通节点，则保存该列表，从列表中选择一个管理节点进行信息索引同步和资源获取路由；如果自己的计算能力值更高，则与列表排名最低的节点通信，交接管理节点位置，拷贝其索引和路由信息，并且广播最新管理节点列表。

[0047] 如果某个集群节点错过了管理节点列表更新，其在连接旧的管理节点时，会被告知最新的管理节点列表。如果排名最低的管理节点无法进行通信，则该节点尝试连接其他管理节点，推荐自己成为管理节点，推荐被接受后，最新管理节点列表也会被广播。如果有管理节点退出网络，与管理节点组协商，更新管理节点列表，普通节点可以根据自身计算能力值，进行推荐提升为管理节点。

[0048] 管理节点保存资源数据，并且在管理节点内进行同步。普通节点不存储资源数据，需要资源时，通过管理节点进行获取。簇内传播时，普通节点将信息转给管理节点，并在管理节点间传递，由管理节点实现信息的传播到各个普通节点。需要全网传播时，由管理节点

实现信息路由到全分布结构化P2P网络。

[0049] 每个区域服务器集群的管理节点间同步本区域的公钥信息。每个节点进入P2P网络前，预设网络接入许可证，该许可证基于节点所属区域、节点类型、节点唯一标识、有效期信息而使用该区域私钥离线加密生成。当节点进入网络时，收到管理节点列表并管理节点建立通信连接后，管理节点需要验证节点唯一标识是否使用过，如果使用过，该唯一标识对应的节点是否在线，如果在线，拒绝该节点连接；如果节点唯一标识有效，验证节点许可证是否有效，管理节点先确认许可证没有被篡改，然后使用公钥解密许可证，确认许可证中的节点唯一标识与目前节点上报的唯一标识一致，有效期可用，如果验证通过，则接受该节点。

[0050] 在本发明的P2P网络中，所有节点都被当作二叉树的叶节点，并且每一个节点的位置都由其ID值唯一的确定。对于二叉树上的每一个节点都可以通过异或操作算出逻辑距离，即在每个节点内保存节点距离路由表，每个路由表内保存多个节点信息(节点地址、端口、节点码)。

[0051] 节点加入全分布结构化网络时进行组播，发布自身节点标识，寻找网络内节点。当前节点接收多个最接近自身节点的节点信息，按照节点标识开始构建自己二叉树和路由表，对二叉树的节点进行查询，直到没有新的节点出现。当节点x收到另一个节点y消息时，发送节点的信息更新对应的路由表和二叉树数据，具体如下：

[0052] 第一，计算节点x和节点y的逻辑距离$d(x,y)=x\oplus y$

[0053] 第二，根据逻辑距离d(x,y)选择对应逻辑距离的路由表进行更新操作。

[0054] 如果节点y已经存在于这个路由表中，则该节点移到这个路由表的尾部，表明这个节点最近被更新过；如果节点y没有记录在这个路由表中，则将它增加到二叉树中，把节点y(节点地址、端口、节点标识)插入该路由表的队列尾部。

[0055] 每个节点周期性的发布全部自己存放数据资源索引，在离自己最近的邻居需要核实资源内容是否更新，选择需要更新的资源进行更新，即使节点在之后失效了，它存放的资源数据也已经被更新到其他新节点上，从而实现任何节点失效，数据都不会丢失。

[0056] 当有社交数据需要传播时，首先计算数据消息的SHA1散列值得到消息摘要，在P2P网络上，这个消息至少需要存储在节点标识和消息摘要一致的节点及靠近它的邻居节点上。具体步骤如下：

[0057] 第一，计算x与消息摘要m的逻辑距离$d(x,m)=x\oplus m$，其中，从节点x的第$\log_2 d(x,m)$个路由表中取出a个节点，如果这个距离的路由表中节点少于a个，则从其他距离的表里选择最接近d(x,m)的节点，向这些节点转发该消息摘要所代表的消息。

[0058] 第二，每个接到转发消息的节点，如果在自己路由表里没有发现更接近消息摘要的节点，则转发结束；否则，继续选择a个节点返回。

[0059] 第三，节点x对收到的a节点都进行消息转发，直到每个分支都有最后回复，则得到a个最接近消息摘要的节点。节点x根据自己建立的二叉树，排除了已经进行消息转发的节点后，向其他节点传播定向消息，接到定向消息的其他节点按照随机距离和随机节点数进行转发。

[0060] 在获取到其他节点的地址之后，节点发送自己的版本信息给对端节点，以尝试建

立连接。该版本信息包括本节点的系统版本、已经同步的区块、节点的当前系统时间。对端节点收到版本信息之后回复自己的版本信息。当双方都获取到对方的版本信息之后，就会发送一个确认信息。尝试建立连接的两个节点在收到对端发过来的版本信息之后，核对系统的时间，确认双方的系统时间是同步的。如果在预设周期内都没有收到对端的心跳信息，则节点将这条链接断开。

[0061] 当一个节点首次加入社交网络区块链系统后，在进行初始化时，节点首先下载网络中最长的区块链上的所有区块数据，本发明通过随机选择网络中的一个节点的方式进行区块同步。被同步节点收到请求之后，按照信息内的请求回复一个头信息。这个头信息包括从首个区块开始的区块链上的所有区块的头信息HASH值。在收到被同步节点回复的头信息之后，新节点会根据共识机制和目标数来判断头信息中头信息HASH值的正确性。之后新的节点再次发送请求头信息去请求接下来的区块头信息HASH值。之后新节点向其他节点重复同样的区块初始化过程。在确认了获取的头信息是属于当前网络中的最优区块链之后，新节点会向网路中的完全节点发送请求数据信息以获取完整的区块信息。

[0062] 所述共识模块用于维护全网数据一致性，每个节点独立地对新区块进行校验并组装进区块链。对于社交网络，考虑到私有链的可信任性，采用基于会话和用户数据的独立校验。具体地，首先根据各个终端发送的记录类型，按社交网络数据记录的约定，写入本次会话内容；输入本节点最新区块HASH值、会话信息属性、加密后的用户属性；验证提交数据更新的终端节点是有效节点；如果验证没有通过，数据写入将被拒绝；每一个输入的解锁脚本必须依据相应输出的锁定脚本来验证；记录本节点最新区块产生时间与验证完毕时间的差值。在收到数据记录后，每一个节点都在全网广播前对这些交易进行校验，并以接收时的相应顺序为有效的新数据块建立一个数据块池。

[0063] 数据块被验证后，集群节点将这些数据块添加到自己的内存池中，用来暂存尚未被加入到区块的记录。在这个过程中，集群节点收集、验证并中继新的会话，并把这些会话整合到一个候选区块中。集群节点记录并校验交易的同时，继续监听社交网络会话，在尝试挖掘新区块的同时，也监听由其他节点发现的区块。

[0064] 构建区块的过程可以分为：第一，集群节点初始化一个未注册候选区块；第二，通过求解工作量证明算法获取记帐权；第三，写入已验证数据块，成为注册正式区块。

[0065] 当产生的新区块通过网络传播之后并在集群节点转发前，需要验证新区块，包括数据结构是否有效，语法是否正确；然后验证新区块父块是否校验正确；新区块的时间戳是否满足早于验证时刻未来的预设时间间隔；最后判断区块内的数据是否满足合规性；如果上述条件均满足，则新区块验证成功，输出校验结果。

[0066] 最后，所述共识模块进行区块链的组装。集群节点在验证新区块后，将新区块连接到当前主链上并组装，首先在区块链中寻找新区块父块；链接新区块，如果当前有效区块未找到父块的，投放到独立区块序列中；从独立区块序列中寻找以新链区块为父块的子块，直接将其链入链上；验证区块内的数据块；如果验证成功，则组装完成。一旦收到了父区块并且将其连接到现有区块链上，节点就从独立区块序列中取出，并且连接到它的父区块，作为区块链的一部分。

[0067] 所述智能合约模块基于社交网络私有区块链，设计部署智能合约，即通过代码的形式定义社交网络通信环节中用户与系统存在的交互的业务过程。编写智能合约包括确认

业务信息的格式、业务状态、业务状态变更的条件、业务状态变更的触发方式、业务状态变更时需要更新的业务信息。代码的编写过程只需要关注业务功能的处理。

[0068] 通过编写的智能合约，用户可以查看和更改对所拥有的社交网络数据记录的访问权限，实现了用户对隐私数据的访问控制；社交网络数据可以在不同节点之间进行安全转移，实现了对隐私数据的保护；集群将对称加密密钥和用户个人属性信息存储至区块链中，用户通过与区块链上的智能合约交互更改属性信息的访问权限和获取加密密钥以解密属性信息。第三方社交平台通过区块链获取用户的信息，使用投票算法决定第三方社交平台的新节点是否具有合法性，基于决定结果实现添加节点、授予权限以及自动注册功能。

[0069] 所述智能合约包括共识合约，共识合约定义了当第三方社交平台有节点发起注册时，区域服务器集群的管理节点验证注册节点是否有效，若该注册节点获得预设比例的区域服务器集群内普通节点的选票则可以加入到系统中，也可以避免重复注册的情况发生。共识合约还可以对合法的节点进行分类，将分类结果和节点地址存储于分类合约中。分类合约存储了所有节点的分类信息，当新节点注册时可先查询分类合约中是否已经存储该节点信息，简化注册过程。

[0070] 所述智能合约包括历史合约、所有关系合约以及访问权限合约。每个用户节点均拥有历史合约，用于存储与本节点有社交联系的节点信息以及所有关系合约的地址。所有关系合约则存储了属性信息拥有者以及访问权限合约的地址，该合约的主要功能就是为了追踪集群存储的数据。用户可通过合约中存储的数据库信息查看自己的数据是否存储在合法的位置，通过查看属性信息的HASH值建立数据完整性。访问权限合约则存储了用户节点的权限信息，根据不同类型的节点定义了相应的权限。初始情况下，所有节点具有密文权限，即只能查看其他节点的属性信息密文。

[0071] 所述智能合约还包括用于二次加密的加密合约，该二次加密用于将属性信息的所有者用户通过集群节点产生针对第三方社交平台节点的转换密钥，该集群节点利用该转换密钥能够将属性信息的所有者用户的公钥加密后的密文转换为第三方社交平台节点用公钥加密后的密文。二次加密过程如下：加密合约首先获取主密钥并向各集群节点发送接受者的公钥，假设有i个集群节点，每个集群节点都生成一个随机数p，记作p_i，分别用主密钥和公钥对p_i加密生成p_i密文对，并将其发送给加密合约。加密合约利用同态乘法运算将加密的p_i整合成随机数p，返回给集群节点，集群节点从中解出转换后消息mp的值，再将消息mp发送给加密合约，合约计算接收者即第三方社交平台节点的新密钥。

[0072] 所述智能合约还包括自动注册合约，此合约中存储了由对称加密密钥加密的用户个人属性信息具体HASH值。第三方社交平台通过访问注册合约中的数值，使用私钥解密获取注册结果，将是否满足注册条件的结果返回给合约，若符合条件则自动将用户以匿名方式注册到第三方社交平台。

[0073] 具体地，第三方社交平台首先向用户发送添加请求，用户向分类合约发送该第三方社交平台的地址，分类合约检索该节点是否已经存在于数据库中，若不存在，将请求的地址和类型发送给共识合约，管理节点验证是否符合请求的分类，投票完成后将结果返回给分类合约，分类合约确认授权，将该第三方社交平台地址和分类结果存储至合约数据库中；若第三方社交平台地址已经存储于分类合约中但存储的分类与要求的分类不一致，则再次对此节点进行投票验证，将投票结果存储至合约中。

[0074] 为保护用户敏感数据的隐私，第三方社交平台只具有读取属性数据记录密文的权限。任何角色添加权限或更改权限都需获得用户同意。在第三方社交平台具有密文权限之后，用户向历史合约获取所有关系合约的地址，再向所有关系合约请求访问权限合约的地址，得到该属性数据记录的访问权限合约地址后向其发送更改第三方社交平台权限请求，访问权限合约检索是否已经存储该节点的信息，若不存在该节点信息则直接将该第三方社交平台节点的地址和请求的权限添加进合约。当集群请求更改第三方社交平台权限时，集群通过访问自己的历史合约找到访问权限合约的地址，访问权限合约检索是否已经存储节点的地址及权限，在访问权限合约确认更改第三方社交平台权限时，首先询问用户是否同意更改，即用户仍拥有属性数据记录的所有权。

[0075] 假设在注册之前第三方社交平台和社交网络区域服务器集群已经约定好使用的加密算法E_{pk}，公私密钥对为(P_k,S_k)，私钥由第三方社交平台保存。自动注册合约创建过程具体如下：

[0076] 1、区域服务器集群将该用户的属性信息存储至分布式数据库。

[0077] 2、集群向第三方社交平台请求该用户的跨平台注册信息；

[0078] 3、第三方社交平台响应请求，将该用户的属性信息分别加密(形式为$E(M_1)$，$E(M_2)$，…，$E(M_n)$)发送给集群，M_i为第i项属性信息；

[0079] 4、集群创建注册合约，计算由对称加密密钥加密的属性数据记录和用户属性数据记录中所记录的属性M的HASH值；计算$E(M_1)\times E(M)^{-1}$，$E(M_2)\times E(M)^{-1}$，…，$E(M_n)\times E(M)^{-1}$，并将计算结果乱序放入属性加密数组中。将用户地址、HASH值以及属性加密数组存储至自动注册合约。

[0080] 此时，当用户发起注册请求时，用户不直接与第三方社交平台交互，而是先向集群发起请求，集群收到请求向第三方社交平台发送自动注册合约的地址。第三方社交平台访问注册合约，获取属性加密数组中的计算结果，使用私钥S_k进行解密。若解密的结果为0，证明2个明文相同，可进行注册；否则拒绝注册。由于第三方社交平台无法辨别究竟是哪个明文与密文匹配，无法获取用户的任何明文属性信息，保证了用户的隐私安全。

[0081] 进一步地，用户地址是由用户公钥生成，通过地址不能推测出用户的身份信息，当第三方社交平台访问注册合约时，并不能通过地址判断用户的身份，即通过智能合约实现了隐藏用户身份信息的功能；其次在注册过程中，第三方社交平台还可以向集群请求加密的属性信息以便与自动注册合约中的HASH值比较，验证数据完整性。

[0082] 综上所述，本发明提出了一种去中心化隐私保护方法，实现了社交网络中用户隐私数据的去中心化存储和认证，认证过程在区块链中完成，利用区块链的不可篡改性确保用户身份的有效性，使用数据摘要代替用户个人信息明文，根据数据摘要为用户匹配信息，即使恶意攻击者截取用户信息也无法查看用户隐私信息明文，保护了用户的隐私。

[0083] 显然，本领域的技术人员应该理解，上述的本发明的各模块或各步骤可以用通用的计算系统来实现，它们可以集中在单个的计算系统上，或者分布在多个计算系统所组成的网络上，可选地，它们可以用计算系统可执行的程序代码来实现，从而，可以将它们存储在存储系统中由计算系统来执行。这样，本发明不限制于任何特定的硬件和软件结合。

[0084] 应当理解的是，本发明的上述具体实施方式仅仅用于示例性说明或解释本发明的原理，而不构成对本发明的限制。因此，在不偏离本发明的精神和范围的情况下所做的任何

修改、等同替换、改进等，均应包含在本发明的保护范围之内。此外，本发明所附权利要求旨在涵盖落入所附权利要求范围和边界、或者这种范围和边界的等同形式内的全部变化和修改例。

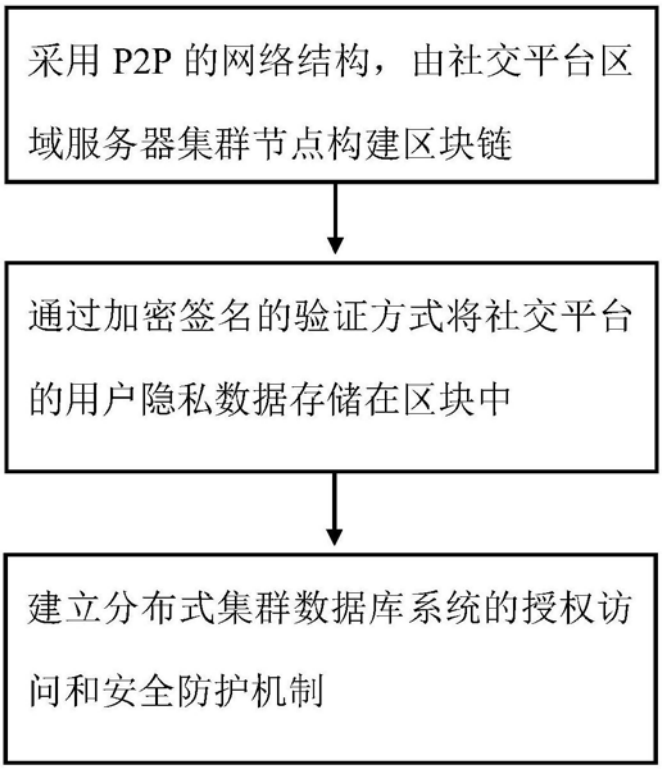

采用 P2P 的网络结构，由社交平台区域服务器集群节点构建区块链
通过加密签名的验证方式将社交平台的用户隐私数据存储在区块中
建立分布式集群数据库系统的授权访问和安全防护机制

图1