(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 109922039 B
(45)授权公告日 2021.05.07

(21)申请号 201910031544.7

(22)申请日 2019.01.14

(65)同一申请的已公布的文献号
申请公布号 CN 109922039 A

(43)申请公布日 2019.06.21

(73)专利权人 湘潭大学
地址 411105 湖南省湘潭市雨湖区羊牯塘街道湘潭大学

(72)发明人 李哲涛 曹纤纤 王建辉 胡翠 惠逸凡 赵文萱 邹瑜峰

(51)Int.Cl.
H04L 29/06(2006.01)
G06F 21/33(2013.01)

(56)对比文件
CN 108234515 A,2018.06.29
CN 108920723 A,2018.11.30
CN 108012582 A,2018.05.08
CN 107018125 A,2017.08.04
CN 108491980 A,2018.09.04
WO 2018120121 A1,2018.07.05
沈鑫,裴庆祺,刘雪峰.“区块链技术综述”.《网络与信息安全学报》.2016,第2卷(第11期),11-20页.
董贵山,陈宇翔,张兆雷,白健,郝尧.“基于区块链的身份管理认证研究”.《计算机科学》.2018,第45卷(第11期),52-59页.
陈维超.“基于区块链的IP版权授权与运营机制研究”.《出版科学》.2018,第26卷(第05期),18-23页.
Okada H , Yamasaki S , Bracamonte V. “Proposed classification of blockchains based on authority and incentive dimensions”.《2017 19th International Conference on Advanced Communication Technology (ICACT). IEEE, 2017》.2017,593-597页.

审查员 王务鹏

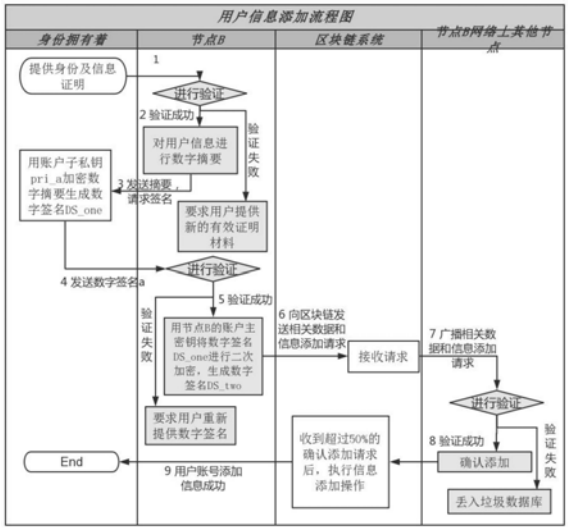
权利要求书2页 说明书7页 附图4页

(54)发明名称

一种基于区块链技术的半中心化的身份管理方法

(57)摘要

本发明提出一种基于区块链技术的半中心化的身份管理方法。首先根据节点信息对节点进行等级划分,分别建立私有区块链,然后结合存储数据类型,划分出多个网络和系统,各个网络节点拥有各自的权限和职责。并通过生成特有的许可证书、利用双重加密算法进行传输和三方确认等方式形成特定的步骤来进行注册、后续信息添加和查询等操作。本发明基于POC信用共识机制,通过引入权限控制体系和双重密钥技术,限制加入节点及其权限的方式将区块链技术应用于身份档案管理领域,通过建立联盟区块链,形成私有区块链网络来管理身份,以期望达到简化身份认证流程,提高用户的主动权,保证档案无法被私自篡改且所有数据都可回溯的目的。



CN 109922039 B

1.基于区块链技术的半中心化的身份管理方法,其特征在于基于POC信用共识机制,通过建立联盟区块链,采用授权控制方法,引入分层确定性钱包技术和双重密钥技术,限制加入节点及其权限的方式将区块链技术应用于身份档案管理领域,形成一个半中心化的可靠的信任体系进行身份管理,至少还包括以下步骤:

步骤1:基于半中心化的思想,根据各节点信息对其进行等级划分:每一个用户即为一个节点,每个节点拥有不同的权限,可依此分为一级节点、二级节点、三级节点和四级节点;一级节点拥有身份管理权限,位于身份管理网络,当一级节点要进行添加自身账户信息或一级节点账户注册操作时需请求其他一级节点进行添加验证和操作,二级节点拥有信息添加权限和查询权限,位于信息添加网络,当二级节点要进行添加自身账户信息操作时需请求一级节点进行验证和操作,三级节点拥有查询权限,位于查询网络,四级节点只有请求添加或查看自身账户的权限,即一级节点之间相互制约,一级节点管理二级节点,二级节点管理三级节点的半中心化管理方法,并分别建立私有区块链,形成多个区块链网络;

步骤2:将各个信息存储模块分开,结合区块链网络划分为多个系统,根据需要存储数据的信息类型将其存于不同的系统中;

步骤3:引入非对称加密技术和双重密钥技术在进行用户注册操作和信息添加操作时进行双方确认,在进行查询操作时进行二次验证。

2.根据权利要求1所述的基于区块链技术的半中心化的身份管理方法,其特征在于所述用户注册操作流程,至少还包括以下步骤:

步骤311:用户向所述身份管理网络中的一级节点请求注册,所述一级节点在验证成功后生成许可证书;

步骤312:用户绑定客户端,发送注册请求;

步骤313:区块链接收请求,向步骤311中所述一级节点发送命令并广播至身份管理网络;

步骤314:所述身份管理网络上的其他节点首先对所述许可证书中的证书头进行验证,然后对许可证书中的数字签名进行验证,全部验证成功后向区块链发送授权信息;

步骤315:区块链接收到所述身份管理网路上超过50%的节点的授权信息后运用分层确定性钱包技术生成账户,并进行用户注册操作;

步骤316:用户获得账户,加入区块链系统。

3.根据权利要求2所述的基于区块链技术的半中心化的身份管理方法,其特征在于:

所述许可证书:用于向区块链获取授权和注册许可,由证书头和数字签名组成;

1)、证书头:所述一级节点使用账户主密钥将自身账户公钥进行加密形成的密文;

2)、数字摘要:把用户的初始注册信息和请求注册的节点的权限等级用安全Hash编码法进行加密后,形成固定长度的密文;

3)、用所述一级节点的账户主密钥对摘要进行加密生成数字签名;

4)、将证书头和数字签名打包,生成许可证书;

5)、每个许可证书都是用户专有的,无法转借给其他用户也无法重复使用。

4.根据权利要求1所述的基于区块链技术的半中心化的身份管理方法,其特征在于所述信息添加操作流程,至少还包括以下步骤:

步骤321:用户向拥有本级用户节点信息添加权限的节点请求信息添加,所述拥有权限

节点生成数字摘要,并发送相关数据至用户账户;

步骤322:用户对所述数字摘要进行验证后,利用非对称加密技术对其进行加密,生成数字签名,并发送回步骤321中所述拥有权限节点;

步骤323:所述拥有权限节点利用非对称加密技术对步骤322中所述数字签名进行加密,形成双重加密数字签名,并发送至区块链系统,同时发送相关信息至所述拥有权限节点所属网络;

步骤324:所述网络上其他节点对所述双重加密数字签名进行验证,并向区块链发送授权信息;

步骤325:区块链接收到所述网络上超过50%的节点的授权信息后进行信息添加操作。

5.根据权利要求1所述的基于区块链技术的半中心化的身份管理方法,其特征在于所述查询操作流程,至少还包括以下步骤:

步骤331:请求查询的节点将查询要素用安全Hash编码法加密生成数字摘要,并使用非对称加密算法对所述数字摘要进行加密生成数字签名,并将查询请求、完整的查询要素和数字签名发送给区块链系统;

步骤332:区块链接收请求,向权力要求1中所述身份管理网络广播上述查询请求、完整的查询要素和数字签名;

步骤333:所述身份管理网络上的节点对查询请求进行验证,并向区块链系统发送确认授权请求和被查询的用户账户信息;

步骤334:区块链接收到所述身份管理网路上超过50%的节点的授权信息后发送查询请求至所述信息添加网络;

步骤335:所述信息添加网络请求进行验证,并向区块链系统发送确认授权请求和被查询的账户的添加信息;

步骤336:区块链接收到所述信息添加网路上超过50%的节点的授权信息后,将收到的数据进行比对验证、整合、打包并发送给步骤331所述请求查询的节点。

一种基于区块链技术的半中心化的身份管理方法

技术领域

[0001] 本发明涉及安全接入技术、区块链技术以及信息安全领域，具体涉及一种基于区块链技术的半中心化的身份管理方法

背景技术

[0002] 随着时代的发展以及与日俱增的数据量，传统的身份管理系统面临着诸多困难。传统中心化身份管理系统采用的是中心化的技术方案，即客户端完全信任服务器。所有用户的信息都存储在中心化数据库中，安全系数和防篡改能力都很低，系统非常容易受到DDOS(distributed denial of service)攻击(即分布式拒绝服务攻击)。身份拥有者(用户)没有身份的管控权利，隐私保护困难，认证流程低效且繁琐。身份管理者(企业等)彼此孤立，且存在利用职权私自篡改用户信息的风险。

[0003] 区块链技术是一种新型的分布式数据库技术，其特点是去中心化、公开透明，让每个成员均可参与数据库的记录。利用区块链技术储存的信息其真实性不容篡改，一旦信息被计入区块链，这个信息就具有不可篡改性和可验证性。其去中心化的特性使我们无需担心因自然灾害、黑客攻击等造成的系统崩溃时的数据丢失。但也使得链上的数据信息和参与节点难以管理，浪费了大量的存储和计算资源。

发明内容

[0004] 针对上述传统方案存在的问题，本发明提出一种基于区块链技术的半中心化的身份管理方法。基于POC(Proof of Credit)信用共识机制，通过引入权限控制体系和双重密钥技术，限制加入节点及其权限的方式将区块链技术应用于身份档案管理领域，通过建立联盟区块链，形成私有区块链网络来管理身份，以期望达到简化身份认证流程，保证档案无法被私自篡改且所有数据都可回溯的目的。

[0005] 具体方案如下：

[0006] 该方案包括：公开系统、身份管理系统、信息添加系统、查询系统和安全系统；

[0007] 公开系统包括：账户公钥库、信息公钥库、空白信息库和垃圾回收库；

[0008] 其中账户公钥库中包含了每个节点的账户公钥，每个账户有且只有一个；

[0009] 信息公钥库包含了每个节点后续添加的信息块的公钥；

[0010] 空白信息库包含了每个账户中未被定义的公钥，每个账户有且只有一个；

[0011] 身份管理系统包括：身份管理网络：由每一个拥有身份管理权限(包括注册账户权限、信息添加权限、查询权限)的节点组成的私有链，该链上的节点拥有身份注册权限、信息添加权限、查询权限和向信息添加网络进行广播的权限；这些节点中备份的区块链中所有用户的账户块；

[0012] 其中账户块包括：区块链序号、许可证书、注册初始信息、进行注册操作的一级节点信息和账户权限信息；

[0013] 信息添加系统包括：信息添加网络：由每一个拥有信息添加权限和查询权限的节

点组成的私有链，该链上的节点拥有信息添加权限和查询权限；这些节点中备份的区块链中所有用户后续添加的信息块；

[0014] 其中信息块包括：区块链序号、添加的信息、进行添加操作的节点信息；

[0015] 查询系统包括：查询网络：由每一个仅拥有信息查询权限的节点组成的私有链，该链上的节点拥有信息查询权限，且只备份自己的账户信息。

[0016] 安全系统：选择记录部分系统操作，如注册账户，增加信息区块，使用查询机制等；定期对系统的各个区块进行审查，若发现异常情况，如某个节点的区块信息与其他节点的不一致，则会向该节点发出警报，同时生成异常日志录入事务表；在接收每个请求之前对发送请求的节点进行异常排查，同时根据节点账户的授权信息与请求操作进行对应，如果节点没有操作权限则向节点发出警告信息，同时生成异常日志录入事务表；定期进行日志分析，当节点的异常行为事件违反或超出正常访问行为的限定时，会从账户库中删除节点，并全网广播。除公开日志外，只有一级节点有访问日志权限，且每一次访问记录都会录入公开日志，公开日志全网可见。

[0017] 节点：每一个用户即为一个节点，每个节点拥有不同的权限，可依此分为一级节点、二级节点、三级节点和四级节点；一级节点拥有身份管理权限，位于身份管理网络。当一级节点要进行添加自身账户信息或一级节点账户注册操作时需请求其他一级节点进行添加验证和操作，二级节点拥有信息添加权限和查询权限，位于信息添加网络。当二级节点要进行添加自身账户信息操作时需请求一级节点进行验证和操作。三级节点拥有查询权限，位于查询网络。四级节点只有请求添加或查看自身账户的权限。即一级节点之间相互制约，一级节点管理二级节点，二级节点管理三级节点的半中心化管理方法。

[0018] 账户主密钥：即种子密钥(种子私钥)。每个账户有且只有一个，与之对应的公钥称作账户公钥。后续添加的信息块私钥都由种子密钥推导产生，即只需备份一个种子密钥即可推导出全部的私钥，亦可根据账户公钥推导出所有的子公钥，从而推导出所有的区块地址，账户运用了分层确定性钱包(Hierachical Deterministic Wallets)技术。

[0019] 许可证书：用于向区块链获取授权和注册许可。由证书头和数字签名组成。

[0020] ————证书头：拥有管理权限的一级节点使用账户主密钥将自身账户公钥进行加密；

[0021] ————数字摘要：把用户的初始注册信息和判定的请求注册的节点的权限等级用安全Hash编码法(SHA:Secure Hash Algorithm)进行加密后，形成固定长度的密文，即摘要(也称为数字指纹)；

[0022] ————用上述一级节点的账户主密钥对摘要进行加密形成数字签名；

[0023] ————将证书头和数字签名打包，生成许可证书；

[0024] ————每个许可证书都是用户专有的，无法转借给其他用户也无法重复使用。

[0025] 本发明一种基于区块链技术的半中心化的身份管理方法的特点是按如下步骤进行：

[0026] 步骤1：基于原始信任录入初始节点信息，根据各节点信息对其进行等级划分，分别建立私有区块链，形成多个区块链网络，其中一级节点形成身份管理网络；二级节点形成信息添加网络；三级节点形成查询网络；四级节点不形成网络，直接加入区块链系统；

[0027] 步骤2：将各个信息存储模块分开，结合区块链网络划分为多个系统。节点账户初

始数据(即账户块)存储于每个一级节点的本地数据库,属身份管理系统;节点账户后续添加的数据(即信息块)存储于每个二级节点的本地数据库,属信息添加系统;三级节点和四级节点只备份自己的账户信息;

[0028] 步骤3:节点注册时需要利用数字摘要技术和非对称加密技术生成许可证书并进行双方确认,然后将注册数据广播至身份管理网络中的其他节点进行检验并授权,超过50%的节点确认授权后,区块链系统生成节点账户,并分别将相关数据进行广播备份,节点加入成功;

[0029] 步骤4:节点信息添加时同样需要用数字摘要技术和非对称加密技术进行双方确认,然后利用双重密钥技术对数据进行加密,再广播至网络中其他节点进行检验并授权,超过50%的节点确认授权后,区块链系统生成信息块,放入相应空白区块链地址中,并分别将相关数据进行广播备份,信息添加成功;

[0030] 步骤5:节点进行信息查询时需要利用数字摘要技术和非对称加密技术进行数据传输,首先将查询信息广播至身份管理网络中进行检验并授权,验证通过后身份管理网络中的节点会发送被查询节点的账户块至区块链系统,超过50%的节点确认授权后,区块链系统会将查询信息广播至信息添加网络中进行检验并授权,验证通过后信息添加网络中的节点会发送被查询节点的各个信息块至区块链系统,超过50%的节点确认授权后,区块链系统对所有收到的账户块和信息块进行比对验证、整合、打包,用非对称加密技术加密最终打包的数据,发送至查询节点。

[0031] 综上所述,本发明的优点如下:

[0032] 1)、用公开系统、身份管理系统、信息添加系统和查询系统将各个数据模块分开,各个节点只需保存备份自己权限以内的数据,有效防止了无端的资源浪费和信息泄露;

[0033] 2)、引入许可证书和权限控制体系,有效控制了节点的数量及来源,各个节点都拥有自己的许可证书和权限,避免了恶意注册导致的过多垃圾数据,提高了资源利用率,同时增加了信任体系的可信任度,也增强了用户信息的隐私保护;

[0034] 3)、基于区块链技术,引入非对称加密技术和双重密钥技术对信息进行加密、传输,系统逻辑非常透明,通过零知识证明的方法提高了账户信息的防篡改能力,解决了传统的中心化身份管理系统中存在的用户没有把握个人数据的主动权,个人信息被篡改而不自知的问题,保障了录入信息的真实性,同时实现了对身份信息操作的追踪和可回溯性,保证了录入信息的可靠性和安全性。

附图说明

[0035] 图1是本方案中的用户注册流程图;

[0036] 图2是本方案中的用户信息添加流程图;

[0037] 图3是本方案中的信息查询流程图;

[0038] 图4是本方案的数据库系统分布图。

[0039] 具体实施方法

[0040] 本发明设计了基于区块链技术的半中心化的身份管理方法,其具体实施方法如下:

[0041] 结合图1,一个未被包含在区块链中的节点请求加入区块链,其身份注册步骤如

下：

[0042] 步骤1：用户(即身份拥有者)向任一拥有身份管理权限的一级节点(如节点A)提供初始身份证明材料，节点A对其材料的真实性和有效性进行验证，并判定其申请的账户权限等级。若验证失败则驳回用户请求，要求用户提供新的有效证明材料；若验证成功则使用节点A的账户主密钥将自身账户公钥进行加密生成证书头；并将用户提供的初始注册信息和判定的请求注册的节点的权限等级进行数字摘要，然后用节点A的账户主密钥对该摘要进行加密生成数字签名，将证书头和数字签名打包生成许可证书，并向用户传回进行数字摘要的原文和许可证书；

[0043] 步骤2：用户对收到的原文进行检验，检验成功后使用节点A的账户公钥对数字签名解密，同时对收到的原文用SHA编码加密产生另一个摘要，将其与s解密后的摘要进行对比，若两者不一致，则请求节点A重新发送许可证书。反之说明传送过程中信息没有被破坏或篡改，验证成功。用户使用许可证书绑定设备，并向区块链发送许可证书和注册请求；

[0044] 步骤3：区块链通过安全系统对请求进行安全检测后接收请求，并向身份管理网络广播注册请求和许可证书，同时向节点A发送命令：要求节点A发送该许可证书对应的完整的用户初始信息和授权等级至身份管理网络；

[0045] 步骤4：身份管理网络上的其他节点在接收到请求后，首先对许可证书的证书头进行验证：使用节点A的账户公钥对证书头进行解密，若解密得到的公钥与节点A的账户公钥相符，则进行步骤5的操作，否则直接将该请求丢入垃圾数据库；

[0046] 步骤5：身份管理网络上的其他节点用节点A的账户公钥对许可证书中的数字签名进行解密，同时对收到的完整的用户初始信息和授权等级用SHA编码加密产生另一个摘要，将其与解密后的摘要进行对比，若两者一致，则说明该许可证书的确是由节点A发出的，且传送过程中信息没有被破坏或篡改。验证通过后，该节点会向区块链系统发送确认授权请求。否则该请求会被丢入垃圾数据库；

[0047] 步骤6：区块链通过安全系统对请求进行安全检测后接收请求，当超过50％的身份管理网络上的一级节点确认授权后，区块链系统将利用用户的初始注册信息生成账户和主密钥，并将主密钥传回用户设备，将账户信息发送至身份管理系统进行备份，同时将账户公钥广播至公开系统中的账户公钥库；

[0048] 步骤7：用户获得账户和主密钥，主密钥自动派生一个私钥pri_a，从而得到公钥pub_a和一个没有存储任何信息的区块地址。该公钥pub_a会自动存储于空白信息库中。

[0049] 结合图2，当一个已经拥有用户账户的节点请求添加和更新自己的账户信息时，其信息添加步骤如下：

[0050] 步骤1：用户向任一拥有本级用户节点信息添加权限的二级(或一级)节点(如：节点B)提供信息证明材料，节点B对其证明材料进行验证，若验证失败则驳回用户请求，要求用户提供新的有效证明材料；若验证成功，则将用户信息用SHA编码加密形成摘要，将摘要和完整的用户信息用用户的账户公钥加密并发送至用户账户请求用户签名；

[0051] 步骤2：用户收到请求后，使用账户主密钥对数据解密，并将完整的用户信息用SHA编码加密形成另一个摘要，将其与接收到的摘要进行比对，比对一致则说明添加信息正确且信息在传输过程中未被破坏或篡改。用户使用账户中的空白区块地址所对应的私钥pri_a加密数字摘要，生成数字签名DS_one，然后发送给节点B；

[0052] 步骤3:节点B使用用户位于空白信息库中的公钥pub_a对数字签名进行解密,解密成功则说明该数字签名的确由用户发出;节点B将解密后的数字摘要和节点B在步骤1中传给用户的数字摘要进行比对,比对一致,则说明用户信息没有被破坏或篡改。否则驳回用户请求,要求用户重新对数字摘要进行签名。全部验证成功后,拥有信息添加权限的节点B将使用自己的主密钥对数字签名DS_one进行加密,形成数字签名DS_two。节点B向区块链系统发送数字签名DS_one、数字签名DS_two、完整的用户添加信息和信息添加请求。

[0053] 步骤4:区块链通过安全系统对请求进行安全检测并确认节点B的权限等级后接收请求,并向信息添加网络(或身份管理网络)广播数字签名DS_one、数字签名DS_two、完整的用户添加信息和信息添加请求。

[0054] 步骤5:信息添加网络(或身份管理网络)上的其他节点在接收到请求后,首先用节点B的账户公钥对数字签名DS_two进行解密,如果解密后得到的数字签名与数字签名DS_one一致,则说明该请求的确由节点B发出。然后用用户位于空白信息库中的公钥pub_a对数字签名DS_one进一步解密得到数字摘要,同时将完整的用户添加信息用SHA编码加密形成另一个数字摘要,将其与解密得到的数字摘要进行比对,如果比对一致则说明该请求的确由该用户发出,且各项信息在传输过程中没有被破坏或篡改,全部验证通过后,该节点会向区块链系统发送确认授权请求。否则该请求会被其他节点丢入垃圾数据库。

[0055] 步骤6:区块链通过安全系统对请求进行安全检测后接收请求,当超过50%的拥有身份添加权限的节点确认授权后,将用户信息放入公钥pub_a对应的区块地址,并发送至信息添加系统进行备份,同时将公钥pub_a广播至公开系统中的信息公钥库。主密钥自动派生一个私钥pri_b,得到公钥pub_b和一个没有存储任何信息的区块地址。该公钥pub_b会替代原来的公钥pub_a的位置,存储于空白信息库中。

[0056] 结合图3,当一个拥有信息查询权限的账户需要查询信息时,其信息查询步骤如下:

[0057] 步骤1:发送查询请求的节点C生成完整的查询信息,包括本账户权限等级、本账户的账户公钥、期望查询账户的账户公钥,并对查询信息用SHA编码加密生成数字摘要,用本账户的账户主密钥对数字摘要进行加密,生成数字签名。将查询请求、完整的查询信息和数字签名发送给区块链系统。

[0058] 步骤2:区块链通过安全系统对请求进行安全检测并确认节点C的权限等级后接收请求,首先向身份管理网络广播查询请求、完整的查询信息和数字签名。

[0059] 步骤3:身份管理网络上的节点在接收到请求后,用节点C的账户公钥对数字签名进行解密,解密成功则说明该数字签名的确是由节点C发出的;然后将完整的查询信息用SHA编码加密生成另一个数字摘要,将其与解密得到的数字摘要进行比对,如果一致则说明查询信息在传递过程中没有被更改。全部验证通过后,在完整的查询信息中找到被查询账户的账户公钥后,向区块链系统发送确认授权请求和被查询的用户账户信息。否则该请求会被丢入垃圾数据库。

[0060] 步骤4:区块链通过安全系统对请求进行安全检测后接收请求和账户数据,在接收到超过50%的节点的授权请求后,向信息添加网络广播查询请求、完整的查询信息和数字签名。

[0061] 步骤5:信息添加网络上的节点使用与步骤3中身份管理网络上的节点同样的方式

对查询请求进行验证，全部验证通过后，在完整的查询信息中找到被查询账户的账户公钥后，根据账户公钥生成所有的子公钥，在本地数据库中依次查找子公钥对应的信息区块进行打包整理，当查找到空白区块地址时停止查找，并向区块链系统发送确认授权请求和打包好的被查询的账户的添加信息。否则该请求会被丢入垃圾数据库。

[0062] 步骤6：区块链通过安全系统对请求进行安全检测后接收请求和信息数据，在接收到超过50％的节点的授权请求后，对收到的所有账户信息和后续添加信息数据进行比对验证，分别找出在所有节点中该部分数据重合度最高的账户块和信息块，并视为最终正确的账户数据，将其整合、打包后用发送查询请求的节点C的账户公钥加密，发送给请求查询的节点C。同时启动安全系统，向数据出现异常的节点发出警报，并生成异常日志录入事务表。

[0063] 本发明的三个实施例如下：

[0064] 实施例1：结合图1，用户注册的具体实施方法如下：

[0065] 步骤1：用户a(即身份拥有者a)向身份管理节点A提供身份证明；

[0066] 步骤2：身份管理节点A验证通过后生成用户专有的许可证书，并将其传给用户a；

[0067] 步骤3：用户a将许可证书与自己的设备进行绑定，并向区块链发送许可证书和注册请求；

[0068] 步骤4：区块链接收请求，向身份管理节点A请求发送完整的用户信息和授权等级至身份管理网络，同时向身份管理网络广播注册请求和许可证书；

[0069] 步骤5：其他身份管理者接收到请求后首先对许可证书中的证书头进行验证，验证成功后对许可证书中的数字签名进行验证，验证成功后向区块链系统发送确认授权请求；

[0070] 步骤6：区块链接收到身份管理网路上超过50％的节点的授权信息后进行用户注册操作，生成用户a的账户和主密钥，并广播用户a的账户公钥至公开系统；

[0071] 步骤7：如图4所示，用户注册成功并获得账户，主密钥自动派生私钥pri_a，得到一个未被定义的公钥pub_a及其对应的空白区块链地址，公钥pub_a自动保存于空白信息库中。

[0072] 实施例2：结合图2，用户信息添加的具体实施方法如下：

[0073] 步骤1：用户a(即身份拥有者a)提供身份信息证明材料给拥有本级节点信息添加权限的节点B；

[0074] 步骤2：节点B验证通过后将用户信息进行数字摘要，并发送给用户a；

[0075] 步骤3：用户a验证完数字摘要后，选择主密钥最后派生的那个私钥pri_a(它对应账户中未被定义的公钥pub_a)加密数字摘要，并生成数字签名DS_one，传回信息添加节点B；

[0076] 步骤4：节点B验证成功后，用自己的账户私钥(即主私钥)对数字签名DS_one进行二次加密，生成数字签名DS_two，并向区块链发送数字签名DS_one、数字签名DS_two、完整的用户添加信息和信息添加请求；

[0077] 步骤5：区块链系统接收请求后，向信息添加网络(或身份管理网络)广播相关数据；

[0078] 步骤6：网络上其他节点验证成功后向区块链系统发送确认添加请求；

[0079] 步骤7：区块链接收到网络上超过50％的节点的确认添加请求后进行用户a的信息添加操作，并广播被定义的公钥pub_a至公开系统；

[0080] 步骤8:如图4所示,用户a的账户中公钥pub_a被定义,主密钥自动派生私钥pri_b,其对应的公钥pub_b替代公钥pub_a在空白信息库中的位置,用户账户信息添加成功。

[0081] 实施例3:结合图3,用户信息查询的具体实施方法如下:

[0082] 步骤1:拥有查询权限的节点C将查询要素进行数字摘要,并使用主密钥对其进行数字签名,将查询请求、完整的查询要素和数字签名发送给区块链系统;

[0083] 步骤2:区块链接收请求后向身份管理网络广播查询请求、完整的查询要素和数字签名;

[0084] 步骤3:身份管理网络上的节点验证通过后返回确认授权请求和被查询的用户账户信息给区块链系统;

[0085] 步骤4:区块链系统接收到身份管理网络上超过50%的节点的授权信息后,广播查询请求、完整的查询要素和数字签名给信息添加网络;

[0086] 步骤5:信息添加网络验证通过后返回确认授权请求和被查询的用户添加信息给区块链系统;

[0087] 步骤6:区块链系统接收到超过50%的节点的授权后,将收到的账户信息和后续添加信息进行验证、整合、打包和加密,发送至节点C;

[0088] 步骤7:查询节点C获得需要查询的信息,查询成功。

[0089] 上述对实施例的描述是为了便于该技术领域的普通技术人员能理解和使用本发明。熟悉本领域技术的人员显然可以容易地对这些实施例做出各种修改,并把在此说明的一般技术原理应用到其他实施例中而不必经过创造性的劳动。因此,本发明不限于上述实施例,本领域技术人员根据本发明的揭示,不脱离本发明范畴所做出的改进和修改都应该在本发明的保护范围之内。

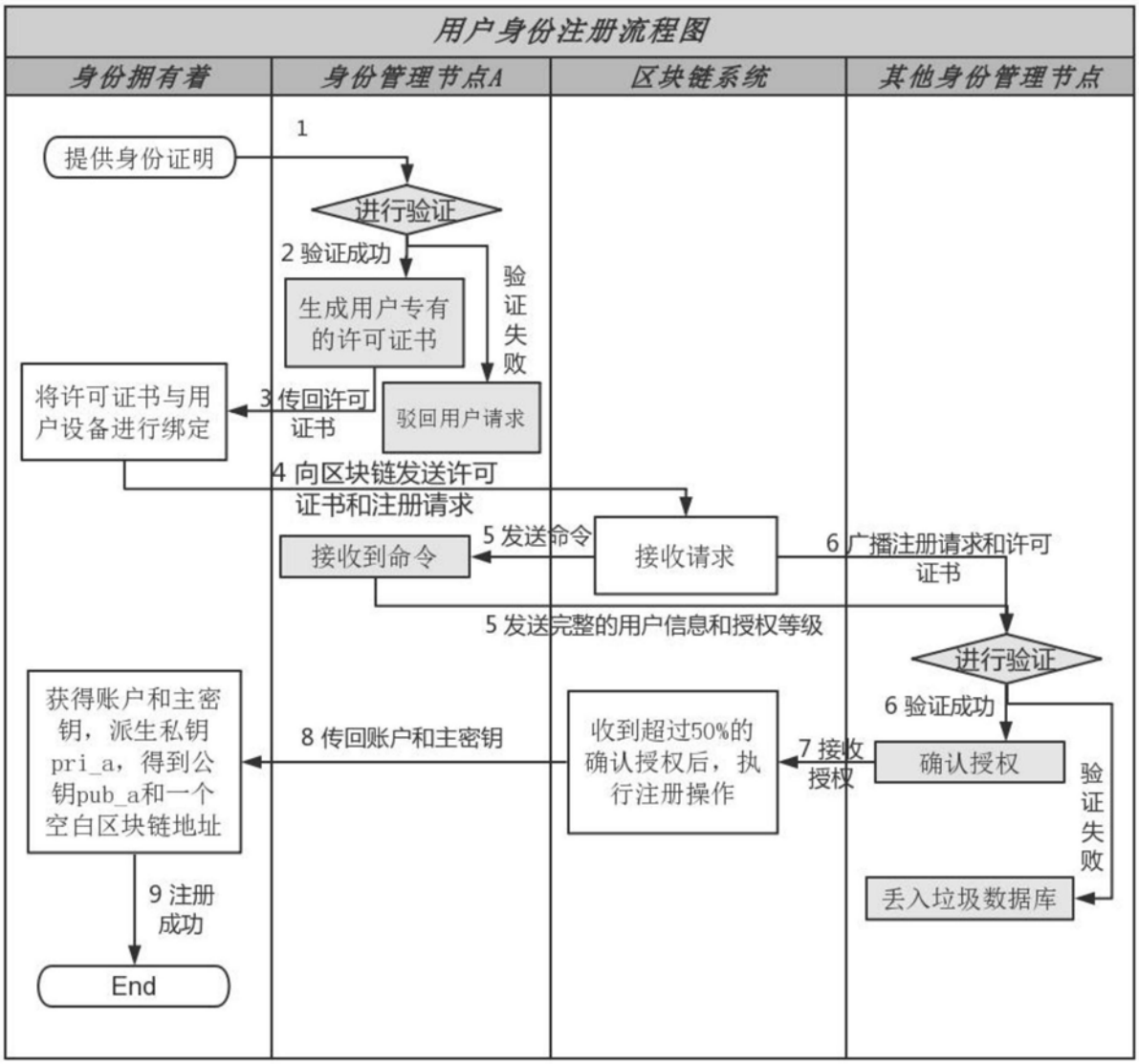

用户身份注册流程图
身份拥有者
身份管理节点A
区块链系统
其他身份管理节点
提供身份证明
1
进行验证
2 验证成功
验证失败
生成用户专有的许可证书
将许可证书与用户设备进行绑定
3 传回许可证书
驳回用户请求
4 向区块链发送许可证书和注册请求
接收到命令
5 发送命令
接收请求
6 广播注册请求和许可证书
5 发送完整的用户信息和授权等级
进行验证
6 验证成功
获得账户和主密钥，派生私钥pri_a，得到公钥pub_a和一个空白区块链地址
8 传回账户和主密钥
收到超过50%的确认授权后，执行注册操作
7 接收授权
确认授权
验证失败
丢入垃圾数据库
9 注册成功
End

图1

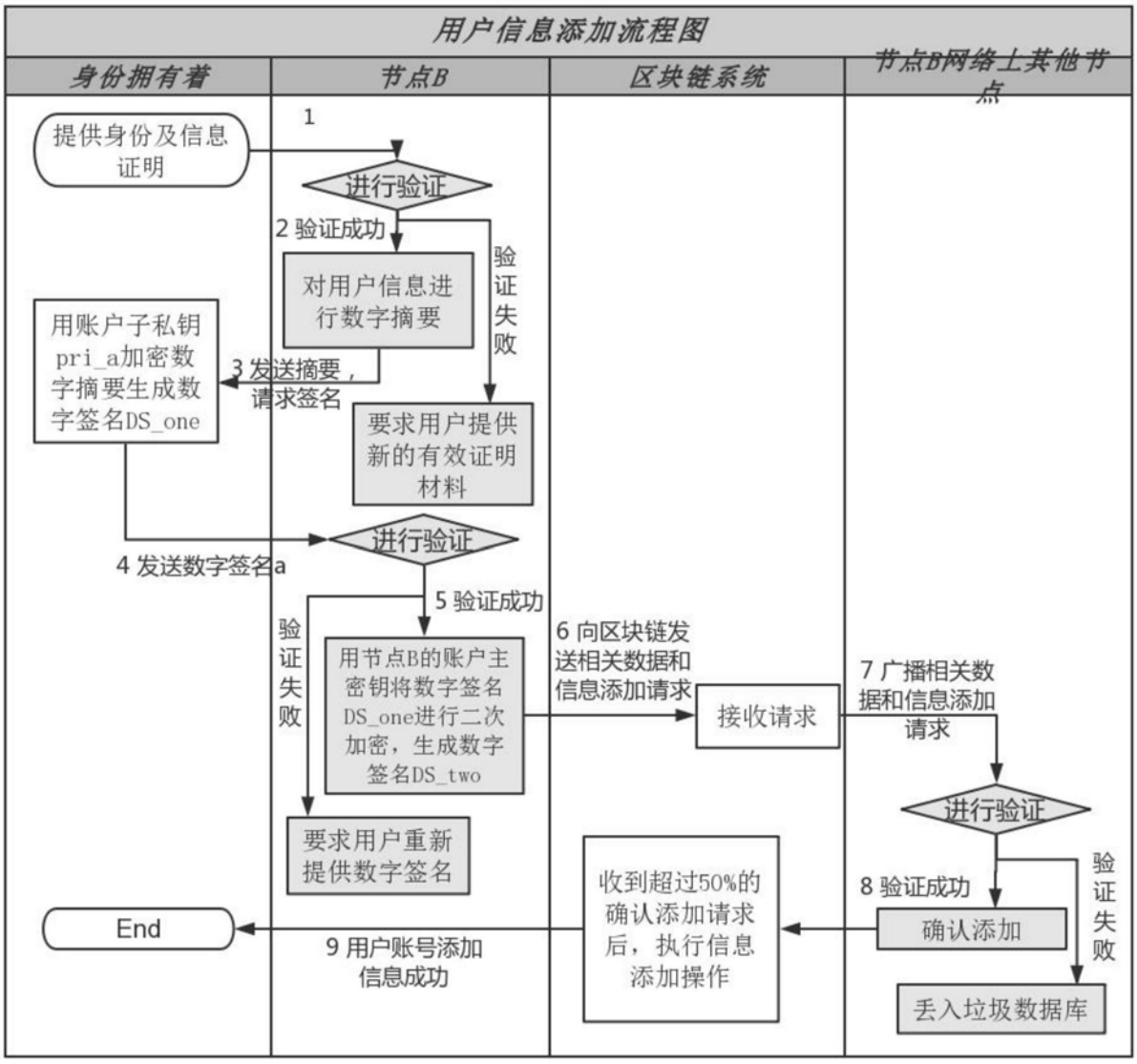

用户信息添加流程图
身份拥有者
节点B
区块链系统
节点B网络上其他节点
提供身份及信息证明
1
进行验证
2 验证成功
验证失败
对用户信息进行数字摘要
用账户子私钥pri_a加密数字摘要生成数字签名DS_one
3 发送摘要，请求签名
要求用户提供新的有效证明材料
进行验证
4 发送数字签名a
5 验证成功
验证失败
用节点B的账户主密钥将数字签名DS_one进行二次加密，生成数字签名DS_two
6 向区块链发送相关数据和信息添加请求
接收请求
7 广播相关数据和信息添加请求
进行验证
8 验证成功
验证失败
确认添加
丢入垃圾数据库
收到超过50%的确认添加请求后，执行信息添加操作
9 用户账号添加信息成功
要求用户重新提供数字签名
End

图2

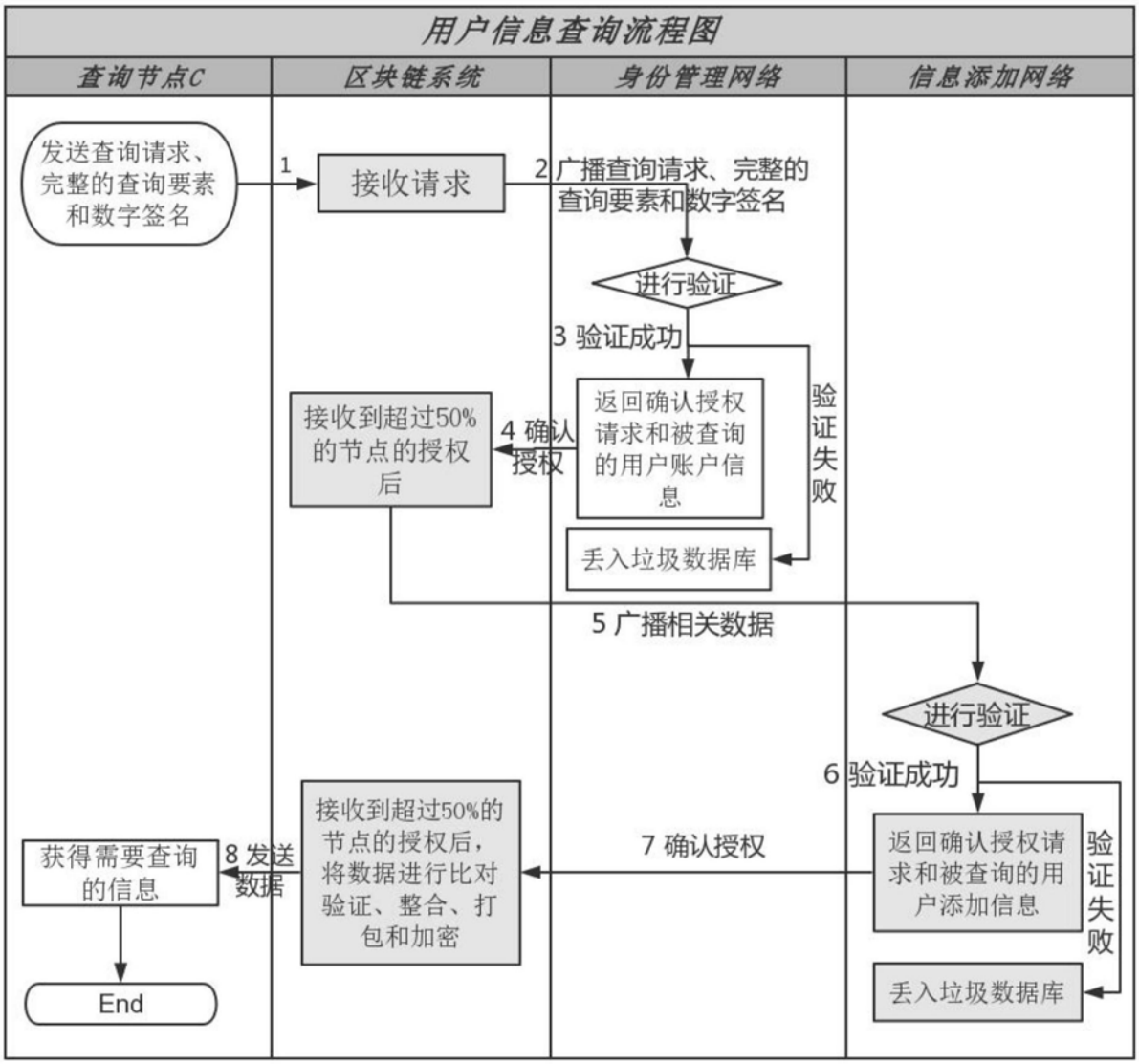

用户信息查询流程图
查询节点C
区块链系统
身份管理网络
信息添加网络
发送查询请求、完整的查询要素和数字签名
1
接收请求
2 广播查询请求、完整的查询要素和数字签名
进行验证
3 验证成功
返回确认授权请求和被查询的用户账户信息
验证失败
丢入垃圾数据库
4 确认授权
接收到超过50%的节点的授权后
5 广播相关数据
进行验证
6 验证成功
返回确认授权请求和被查询的用户添加信息
验证失败
丢入垃圾数据库
7 确认授权
接收到超过50%的节点的授权后，将数据进行比对验证、整合、打包和加密
8 发送数据
获得需要查询的信息
End

图3

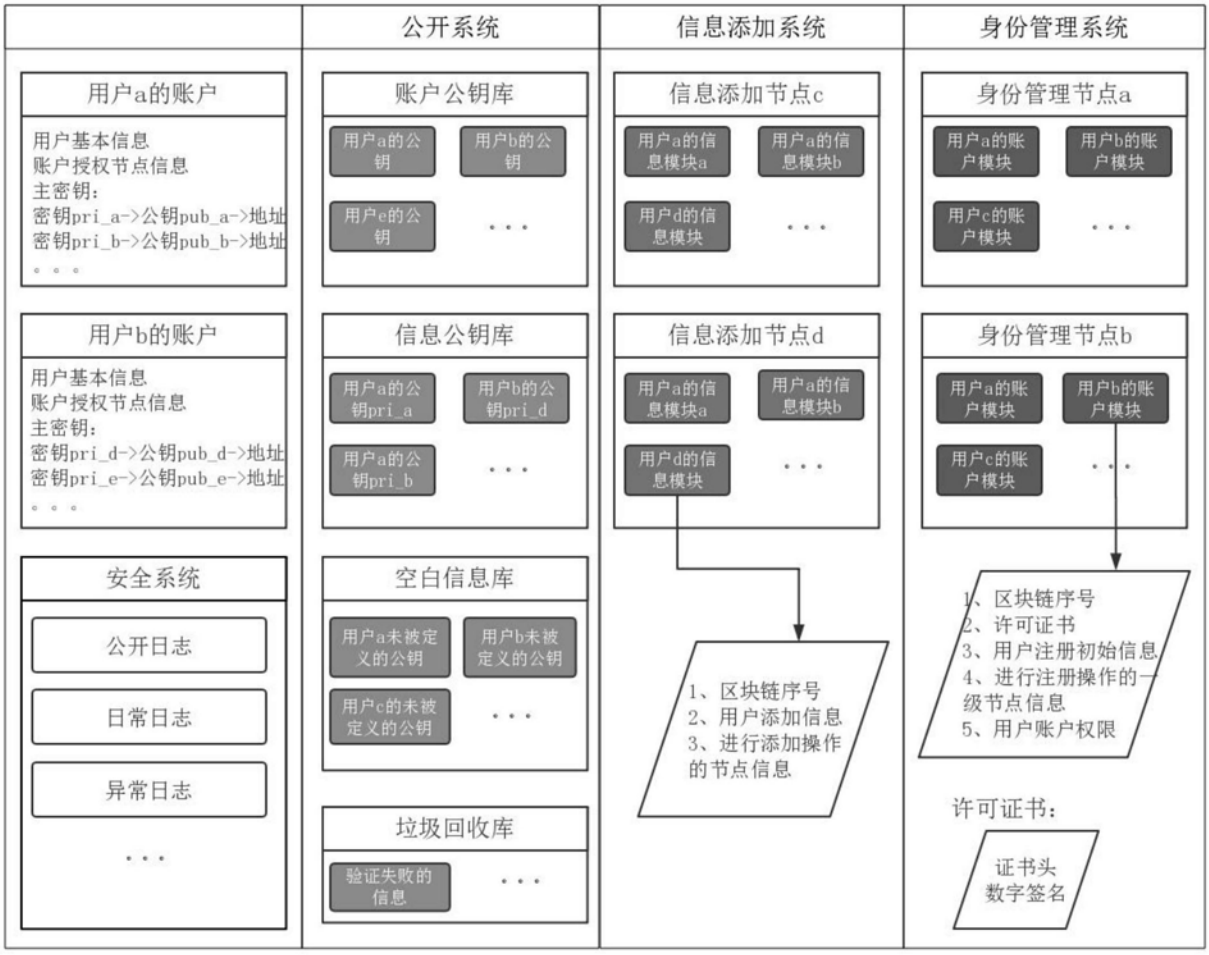

公开系统
信息添加系统
身份管理系统
用户a的账户
用户基本信息
账户授权节点信息
主密钥：
密钥pri_a->公钥pub_a->地址
密钥pri_b->公钥pub_b->地址
用户b的账户
用户基本信息
账户授权节点信息
主密钥：
密钥pri_d->公钥pub_d->地址
密钥pri_e->公钥pub_e->地址
安全系统
公开日志
日常日志
异常日志
账户公钥库
用户a的公钥
用户b的公钥
用户e的公钥
信息公钥库
用户a的公钥pri_a
用户b的公钥pri_d
用户a的公钥pri_b
空白信息库
用户a未被定义的公钥
用户b未被定义的公钥
用户c的未被定义的公钥
垃圾回收库
验证失败的信息
信息添加节点c
用户a的信息模块a
用户a的信息模块b
用户d的信息模块
信息添加节点d
用户a的信息模块a
用户a的信息模块b
用户d的信息模块
1、区块链序号
2、用户添加信息
3、进行添加操作的节点信息
身份管理节点a
用户a的账户模块
用户b的账户模块
用户c的账户模块
身份管理节点b
用户a的账户模块
用户b的账户模块
用户c的账户模块
1、区块链序号
2、许可证书
3、用户注册初始信息
4、进行注册操作的一级节点信息
5、用户账户权限
许可证书：
证书头
数字签名

图4