(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 114189341 B
(45)授权公告日 2024.08.23

(21)申请号 202111506912.2

(22)申请日 2021.12.10

(65)同一申请的已公布的文献号
申请公布号 CN 114189341 A

(43)申请公布日 2022.03.15

(73)专利权人 北京泰尔英福科技有限公司
地址 101399 北京市顺义区中关村科技园区顺义园机场东路8号

(72)发明人 李慧玲 张发振 李龙 柳京晖 武莹 杨树梅 胡键伟 马晨光 曾西平

(74)专利代理机构 北京三友知识产权代理有限公司 11127
专利代理师 薛平 郝博

(51)Int.Cl.
H04L 9/32(2006.01)

(56)对比文件
刘亚雪等.一种基于区块链的多应用证书系统模型.《计算机工程》.2020,46(9),正文第2节.

审查员 楼芃雯

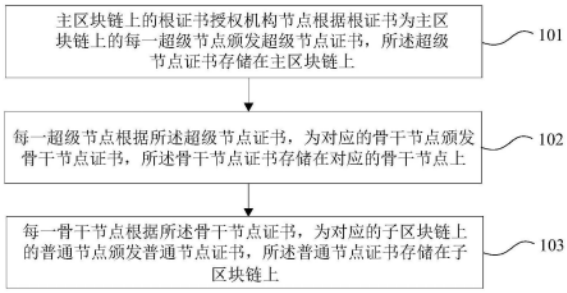
权利要求书2页 说明书9页 附图5页

(54)发明名称

基于区块链标识的数字证书分级处理方法及装置

(57)摘要

本发明公开了一种基于区块链标识的数字证书分级处理方法及装置,根证书授权机构节点和多个超级节点构成主区块链,与每一超级节点连接的一个骨干节点和多个普通节点构成至少一个子区块链,其中该方法包括:根证书授权机构节点根据根证书为每一超级节点颁发超级节点证书,超级节点证书存储在主链上;每一超级节点根据超级节点证书为骨干节点颁发骨干节点证书,骨干节点证书存储在对应的骨干节点上;每一骨干节点根据骨干节点证书为子区块链上的普通节点颁发普通节点证书,普通节点证书存储在子区块链上。本发明采用基于主子链架构的区块链做数字证书身份处理,可以减轻单链负担,提高证书颁发及后续验证性能,实现了高效安全地分级处理数字证书。



CN 114189341 B

1.一种基于区块链标识的数字证书分级处理方法,其特征在于,根证书授权机构节点和多个超级节点构成主区块链,与每一所述超级节点连接的一个骨干节点和多个普通节点构成至少一个子区块链,所述基于区块链标识的数字证书分级处理方法包括:

主区块链上的根证书授权机构节点根据根证书为主区块链上的每一超级节点颁发超级节点证书,所述超级节点证书存储在主区块链上;

每一超级节点根据所述超级节点证书,为对应的骨干节点颁发骨干节点证书,所述骨干节点证书存储在对应的骨干节点上;

每一骨干节点根据所述骨干节点证书,为对应的子区块链上的普通节点颁发普通节点证书,所述普通节点证书存储在子区块链上;

其中,根证书授权机构CA的选定过程包括:

单个CA,中心化的方式,CA内置,不用选;

多个CA通过共识给用户颁发证书,CA的选定方式可以利用信任锚的选择方式;

CA获取自身的证书的过程:

如只有一个CA,可自签证书;

如有多个CA,其他CA给该CA颁发证书:

可在其他有效的CA中随机选择一个颁发证书;

或者在M个有效的CA中选择N个,作为颁发证书的CA。

2.如权利要求1所述的基于区块链标识的数字证书分级处理方法,其特征在于,还包括:

接收当前数字证书的验证请求;

验证所述当前数字证书颁发者的签名;

若根据当前数字证书颁发者的签名验证结果,确定当前数字证书存在上一级颁发者时,验证上一级颁发者的签名,直到找到最初的证书颁发者;所述最初的证书颁发者为根证书授权机构节点;

如果当前数字证书颁发者到最初的证书颁发者的链条上的数字证书验证均为可信,确定当前数字证书可信。

3.如权利要求1所述的基于区块链标识的数字证书分级处理方法,其特征在于,还包括:在检测到根证书、超级节点证书、骨干节点证书和普通节点证书其中的任一级别的证书更新时,更新当前更新证书的下一级证书。

4.如权利要求1所述的基于区块链标识的数字证书分级处理方法,其特征在于,还包括:在检测到根证书、超级节点证书、骨干节点证书和普通节点证书其中的任一级别的证书过期时,向当前过期证书的颁发者重新申请数字证书。

5.如权利要求1所述的基于区块链标识的数字证书分级处理方法,其特征在于,还包括:在检测到上一级用户证书注销后,当前用户证书链条上以下级别用户证书均要注销,需要重新申请。

6.一种基于区块链标识的数字证书分级处理装置,其特征在于,根证书授权机构节点和多个超级节点构成主区块链,与每一所述超级节点连接的一个骨干节点和多个普通节点构成至少一个子区块链,所述基于区块链标识的数字证书分级处理装置包括:

主区块链上的根证书授权机构节点,用于根据根证书为主区块链上的每一超级节点颁

发超级节点证书,所述超级节点证书存储在主区块链上;

每一超级节点,用于根据所述超级节点证书,为对应的骨干节点颁发骨干节点证书,所述骨干节点证书存储在对应的骨干节点上;

每一骨干节点,用于根据所述骨干节点证书,为对应的子区块链上的普通节点颁发普通节点证书,所述普通节点证书存储在子区块链上;

其中,根证书授权机构CA的选定过程包括:

单个CA,中心化的方式,CA内置,不用选;

多个CA通过共识给用户颁发证书,CA的选定方式可以利用信任锚的选择方式;

CA获取自身的证书的过程:

如只有一个CA,可自签证书;

如有多个CA,其他CA给该CA颁发证书:

可在其他有效的CA中随机选择一个颁发证书;

或者在M个有效的CA中选择N个,作为颁发证书的CA。

7.如权利要求6所述的基于区块链标识的数字证书分级处理装置,其特征在于,所述根证书授权机构节点、超级节点、骨干节点或普通节点还用于:

接收当前数字证书的验证请求;

验证所述当前数字证书颁发者的签名;

若根据当前数字证书颁发者的签名验证结果,确定当前数字证书存在上一级颁发者时,验证上一级颁发者的签名,直到找到最初的证书颁发者;所述最初的证书颁发者为根证书授权机构节点;

如果当前数字证书颁发者到最初的证书颁发者的链条上的数字证书验证均为可信,确定当前数字证书可信。

8.一种计算机设备,包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序,其特征在于,所述处理器执行所述计算机程序时实现权利要求1至5任一所述方法。

9.一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计算机程序,所述计算机程序被处理器执行时实现权利要求1至5任一所述方法。

10.一种计算机程序产品,其特征在于,所述计算机程序产品包括计算机程序,所述计算机程序被处理器执行时实现权利要求1至5任一所述方法。

基于区块链标识的数字证书分级处理方法及装置

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标识的数字证书分级处理方法及装置。

背景技术

[0002] 本部分旨在为权利要求书中陈述的本发明实施例提供背景或上下文。此处的描述不因为包括在本部分中就承认是现有技术。

[0003] 由于Internet网电子商务系统技术使在网上购物的顾客能够极其方便轻松地获得商家和企业的信息,但同时也增加了对某些敏感或有价值的数据被滥用的风险。为了保证互联网上电子交易及支付的安全性和保密性等,防范交易及支付过程中的欺诈行为,必须在网上建立一种信任机制。这就要求参加电子商务的买方和卖方都必须拥有合法的身份,并且在网上能够有效无误地被进行验证。

[0004] 关于身份和数字身份的定义:

[0005] 1.身份:一种以一个或多个属性表示的实体,它允许实体在上下文中得到充分的区分。

[0006] 身份是对主体对象的一组属性描述,具有区别性和证明性。区别性在于通过身份的部分或者全部属性信息能够唯一确定一个主体对象,证明性在于通过主体对象的部分或者全部属性信息能够证明主体对象的身份。

[0007] 2.数字身份:一个数字身份是一个实体在数字环境中的数字表示,使得个体在数字环境中能被充分区分。

[0008] 数字身份继承了身份的各种特性,在数字社会中广泛应用,同时也能映射到现实社会中进行应用。绝大多数数字身份都有一个ID属性,用以唯一标识该数字身份,这个ID属性可以是按照某种规则定义生成的一串码,也可以是通过哈希运算生成的一串码,在一定的数字区域里面具有唯一性。

[0009] 如图1所示,一般数字身份会被定义为与一个标识关联的属性集合。也可以是单一的标识,能在环境中唯一区分其表示的实体即可。

[0010] 数字证书是一种权威性的电子文档,是数字身份的一种。它提供了一种在Internet上验证身份的方式,其作用类似于司机的驾驶执照或日常生活中的身份证。它是由一个由权威机构----CA证书授权(Certificate Authority)中心发行的,人们可以在互联网交往中用它来识别对方的身份。当然在数字证书认证的过程中,证书认证中心(CA)作为权威的、公正的、可信赖的第三方,其作用是至关重要的。

[0011] 目前的数字证书类型主要包括:个人数字证书、单位数字证书、单位员工数字证书、服务器证书、VPN证书、WAP证书、代码签名证书和表单签名证书。传统数字证书的颁发和验证依赖于中心化的CA机构,身份数据容易被篡改,存在数字证书处理效率和安全性都低的问题。

发明内容

[0012] 本发明实施例提供一种基于区块链标识的数字证书分级处理方法,用以高效安全地进行数字证书的分级处理,根证书授权机构节点和多个超级节点构成主区块链,与每一所述超级节点连接的一个骨干节点和多个普通节点构成至少一个子区块链,该方法包括:

[0013] 主区块链上的根证书授权机构节点根据根证书为主区块链上的每一超级节点颁发超级节点证书,所述超级节点证书存储在主区块链上;

[0014] 每一超级节点根据所述超级节点证书,为对应的骨干节点颁发骨干节点证书,所述骨干节点证书存储在对应的骨干节点上;

[0015] 每一骨干节点根据所述骨干节点证书,为对应的子区块链上的普通节点颁发普通节点证书,所述普通节点证书存储在子区块链上。

[0016] 本发明实施例还提供一种基于区块链标识的数字证书分级处理装置,用以高效安全地进行数字证书的分级处理,根证书授权机构节点和多个超级节点构成主区块链,与每一所述超级节点连接的一个骨干节点和多个普通节点构成至少一个子区块链,该装置包括:

[0017] 主区块链上的根证书授权机构节点,用于根据根证书为主区块链上的每一超级节点颁发超级节点证书,所述超级节点证书存储在主区块链上;

[0018] 每一超级节点,用于根据所述超级节点证书,为对应的骨干节点颁发骨干节点证书,所述骨干节点证书存储在对应的骨干节点上;

[0019] 每一骨干节点,用于根据所述骨干节点证书,为对应的子区块链上的普通节点颁发普通节点证书,所述普通节点证书存储在子区块链上。

[0020] 本发明实施例还提供一种计算机设备,包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序,所述处理器执行所述计算机程序时实现上述基于区块链标识的数字证书分级处理方法。

[0021] 本发明实施例还提供一种计算机可读存储介质,所述计算机可读存储介质存储有计算机程序,所述计算机程序被处理器执行时实现上述基于区块链标识的数字证书分级处理方法。

[0022] 本发明实施例还提供一种计算机程序产品,所述计算机程序产品包括计算机程序,所述计算机程序被处理器执行时实现上述基于区块链标识的数字证书分级处理方法。

[0023] 本发明实施例中,基于区块链标识的数字证书分级处理方案,根证书授权机构节点和多个超级节点构成主区块链,与每一所述超级节点连接的一个骨干节点和多个普通节点构成至少一个子区块链,与现有技术中传统数字证书的颁发和验证依赖于中心化的CA机构,身份数据容易被篡改,存在数字证书处理效率和安全性都低的问题的技术方案相比,通过:主区块链上的根证书授权机构节点根据根证书为主区块链上的每一超级节点颁发超级节点证书,所述超级节点证书存储在主区块链上;每一超级节点根据所述超级节点证书,为对应的骨干节点颁发骨干节点证书,所述骨干节点证书存储在对应的骨干节点上;每一骨干节点根据所述骨干节点证书,为对应的子区块链上的普通节点颁发普通节点证书,所述普通节点证书存储在子区块链上,采用基于主子链架构的区块链做数字证书身份处理,可以减轻单链负担,提高证书颁发及后续验证性能,实现了高效安全地分级处理数字证书。

附图说明

[0024] 为了更清楚地说明本发明实施例或现有技术中的技术方案,下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍,显而易见地,下面描述中的附图仅仅是本发明的一些实施例,对于本领域普通技术人员来讲,在不付出创造性劳动的前提下,还可以根据这些附图获得其他的附图。在附图中:

[0025] 图1为本发明实施例中数字身份结构示意图;

[0026] 图2为现有技术中基于区块链标识的用户证书申请和使用的示意图;

[0027] 图3为本发明实施例中基于区块链标识的数字证书分级处理方法的流程示意图;

[0028] 图4为本发明实施例中基于区块链标识的数字证书分级颁发处理装置的结构示意图;

[0029] 图5为本发明实施例中基于区块链标识的数字证书分级验证处理示意图;

[0030] 图6为本发明实施例中基于区块链标识的数字证书分级处理的整体流程示意图;

[0031] 图7为本发明实施例中企业及用户证书颁发处理的示意图;

[0032] 图8为本发明实施例中企业及用户证书颁发及验证的整体流程示意图。

具体实施方式

[0033] 为使本发明实施例的目的、技术方案和优点更加清楚明白,下面结合附图对本发明实施例做进一步详细说明。在此,本发明的示意性实施例及其说明用于解释本发明,但并不作为对本发明的限定。

[0034] 在介绍本发明实施例之前,首先对本发明涉及的名词进行介绍。

[0035] eID---Electronic Identity公民网络电子身份标识。

[0036] uport---分布式网络设计的开放式身份系统。

[0037] WAP---Wireless Application Protocol无线应用协议。

[0038] VPN------Virtual Private Network虚拟专用网络。

[0039] BID---Blockchain-based Identifier区块链标识。

[0040] 下面对发明人发现现有数字证书处理存在的技术问题及提出本发明的思路进行介绍。

[0041] 传统方式采用中心化的身份管理方式。数字证书颁发过程一般为:用户首先产生自己的密钥对,并将公共密钥及部分个人身份信息传送给认证中心(CA)。认证中心在核实身份后,将执行一些必要的步骤,以确信请求确实由用户发送而来,然后,认证中心将发给用户一个数字证书,该证书内包含用户的个人信息和他的公钥信息,同时还附有认证中心的签名信息。用户就可以使用自己的数字证书进行相关的各种活动。数字证书由独立的证书发行机构发布。数字证书各不相同,每种证书可提供不同级别的可信度。

[0042] 传统方式采用中心化的身份管理方式,即传统数字证书的颁发和验证依赖于中心化的CA机构,身份数据容易被篡改,存在安全问题。

[0043] 基于区块链标识的身份认证,如eID,uport等,如图2所示,以用户证书申请和使用为例,过程如下:

[0044] 1.用户通过客户端或浏览器注册身份,客户端或浏览器插件为其生成。

[0045] 2.用户将身份激活到链上。

[0046] 3.用户上传身份信息,申请身份凭证。

[0047] 4.信任锚生成身份凭证,并将凭证存储在链上。

[0048] 5.第三方用户请求验证身份凭证。

[0049] 6.用户提供身份凭证并经过黑盒处理,生成可验证数据。

[0050] 7.第三方用户去链上验证身份是否过期。

[0051] 8.链上将用户提供的数据与链上数据比对,进行身份验证。

[0052] 9.链将验证结果返回给用户和第三方用户。

[0053] 因此,基于区块链标识的身份认证技术,数字证书的颁发依赖中心化CA机构,验证过程依赖去中心化的区块链账本。

[0054] 现有基于区块链标识的身份认证多采用扁平化的身份认证方式,即所有的用户在一条链上进行身份认证,对链的性能要求较高,在区块链性能一定的前提下,容易发生堵塞,导致认证时延大。

[0055] 考虑到上述技术问题,本发明提出了一种基于区块链标识的数字证书分级处理方案,该方案:

[0056] 1.采用基于主子链架构的区块链做身份管理,减轻单链负担,提高证书颁发、验证性能。

[0057] 2.采用多级证书验证的方式,在不减少可信度的前提下,减轻根CA负担。

[0058] 3.采用去中心化根CA与中心化系统相结合的方式,中心化系统的根CA在区块链上,减少根CA被篡改的风险。

[0059] 下面对该基于区块链标识的数字证书分级处理方案进行详细介绍。

[0060] 图3为本发明实施例中基于区块链标识的数字证书分级处理方法的流程示意图,根证书授权机构节点和多个超级节点构成主区块链,与每一所述超级节点连接的一个骨干节点和多个普通节点构成至少一个子区块链,如图3所示,该方法包括如下步骤:

[0061] 步骤101:主区块链上的根证书授权机构节点根据根证书为主区块链上的每一超级节点颁发超级节点证书,所述超级节点证书存储在主区块链上;

[0062] 步骤102:每一超级节点根据所述超级节点证书,为对应的骨干节点颁发骨干节点证书,所述骨干节点证书存储在对应的骨干节点上;

[0063] 步骤103:每一骨干节点根据所述骨干节点证书,为对应的子区块链上的普通节点颁发普通节点证书,所述普通节点证书存储在子区块链上。

[0064] 具体实施时,采用基于主子链架构的区块链做证书管理:链上含超级节点、骨干节点、普通节点、用户,被授予证书的主体是链上的节点,证书颁发过程如下图3所示,主要包括:

[0065] 0.前提条件:证书颁发者和证书被授予者都有用户ID(BID),证书颁发者持有证书。

[0066] 1.主链(见图4中的主链,即主区块链)上的根CA(根证书授权机构)节点给主链上的超级节点颁发超级节点证书,发超级节点证书存储在主链上,即上述步骤101,对应附图4中的①。

[0067] 2.超级节点为骨干节点颁发下一级证书(骨干节点证书),骨干节点证书存储在骨干节点上,即上述步骤102,对应附图4中的②。

[0068] 3.骨干节点为子链上的节点颁发下一级证书(普通节点证书),普通节点证书存储在子链(见图4中的子链,即子区块链)上,即上述步骤103,对应附图4中的③。

[0069] 具体实施时,本发明实施例还可以在横向和纵向上延伸更多级别的节点。可以纵向和横向拓展,比如,纵向可以对接更多链横向(对每一条链来说)可以有更多节点类型。

[0070] 具体实施时,本发明实施例中数字证书的类型可以包括:个人数字证书、单位数字证书、单位员工数字证书、服务器证书、VPN证书、WAP证书、代码签名证书和表单签名证书等。

[0071] 本发明实施例提供的基于区块链标识的数字证书分级处理方法采用基于主子链架构的区块链做身份管理,证书既可以在主链上颁发,也可以在子链上颁发,减轻主链负担,提高证书颁发及后续验证性能,实现了高效安全地分级处理数字证书。下面对该基于区块链标识的数字证书分级处理方法进行详细介绍。

[0072] 在一个实施例中,基于区块链标识的数字证书分级处理方法还可以包括:

[0073] 接收当前数字证书的验证请求;

[0074] 验证所述当前数字证书颁发者的签名;

[0075] 若根据当前数字证书颁发者的签名验证结果,确定当前数字证书存在上一级颁发者时,验证上一级颁发者的签名,直到找到最初的证书颁发者;所述最初的证书颁发者为根证书授权机构节点;

[0076] 如果当前数字证书颁发者到最初的证书颁发者的链条上的数字证书验证均为可信,确定当前数字证书可信。

[0077] 具体实施时,如图5所示,以当前数字证书为普通节点证书为例说明数字证书的验证过程:接收当前数字证书的验证请求,即在需要根据数字证书进行身份验证时,例如用户通过普通节点登录系统时或在网上购物时,需要验证用户身份时发起验证请求;验证所述当前数字证书颁发者(例如验证普通节点对应的骨干节点)的签名;若根据当前数字证书颁发者的签名验证结果,确定当前数字证书存在上一级颁发者(超级节点)时,验证上一级颁发者的签名,直到找到最初的证书颁发者;所述最初的证书颁发者为根证书授权机构节点;如果当前数字证书颁发者到最初的证书颁发者的链条上的数字证书验证均为可信,确定当前数字证书(普通节点证书)可信。与图4中过程相反,图5中验证的过程反过来,详见图5中带圆圈数字的标注。

[0078] 具体实施时,基于区块链标识的数字证书分级处理即颁发及验证的整体流程如图6所示。

[0079] 具体实施时,被授予证书的用户可以是个人用户、企业用户或节点用户,其中:

[0080] 1.节点用户可以为节点用户、企业用户或个人用户颁发证书。

[0081] 2.企业用户可以为个人用户颁发证书。

[0082] 3.颁发的证书类型根据CA的类型确定。

[0083] 具体实施时,企业及用户证书颁发过程可以如图7所示,企业及用户证书颁发及验证的整体过程如图8所示。

[0084] 具体实施时,CA的选定过程可以包括:

[0085] 方案1-1:单个CA,中心化的方式,CA内置,不用选;

[0086] 方案1-2:多个CA通过共识给用户颁发证书,CA的选定方式可以利用信任锚的选择

方式。

[0087] 具体实施时,CA获取自身的证书的过程:

[0088] 1.如只有一个CA,可自签证书;

[0089] 2.如有多个CA,其他CA给该CA颁发证书:

[0090] 1)可在其他有效的CA中随机选择一个颁发证书;

[0091] 2)或者在M个有效的CA中选择N个,作为颁发证书的CA。

[0092] 具体实施时,证书内容:CA给其他用户颁发证书,内容包括:证书id、证书类型、证书颁发者id、颁发时间、所有者的id、公钥的失效期、签名日期、证书发放目的、公钥标识、发放机构的数字签名。根据需要证书内容还可能包括被授予证书者的地理位置、名称等字段。一个示例如下表1所示:

[0093]

```
{
// set the context, which establishes the special terms we will be using
 // such as 'issuer' and 'alumniOf'.
"@context": [
"https://www.w3.org/2018/credentials/v1",
"https://www.w3.org/2018/credentials/examples/v1"
],
// 证书id
"id": "did:bid:cc:0x123456789012340000",
// 证书内容格式
"type": ["VerifiableCredential", "AlumniCredential"],
// 证书颁发者
"issuer": " did:bid:cc:0x123456789012340001 ",
 // 证书颁发时间
 "issuanceDate": "2010-01-01T19:73:24Z",
// 被声明者
"credentialSubject":
{ // 被声明者id
 "id": "did:bid: 0x123456789012340002",
// 声明内容
"name": [
{ "value": "Example Node", "lang": "en" },
] } },
 // 数字签名，防篡改
"proof":
{ //加密算法
 "type": "RsaSignature2018",
// 签名生成的日期
"created": "2017-06-18T21:19:10Z",
 // 创建目的：证明
"proofPurpose": "assertionMethod",
// 创建者公钥，用户验证签名
"verificationMethod": "https://example.edu/issuers/keys/1",
// 数字签名值
"jws": "eyJhbGciOiJSUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0II19..TCYt5X sITJX1CxPCT8yAV-
TVkIEq_PbChOMqsLfRoPsnsgw5WEuts01mq-pQy7UJiN5mgRxD-WUc X16dUEMGlv50aqzpqh4Qktb3rk-
BuQy72IFLOqV0G_zS245-kronKb78cPN25DGlcTwLtj PAYuNzVBAh4vGHSrQyHUdBBPM" } }
```

[0094] 表1

[0095] 下面介绍本发明实施例进一步优选的步骤,即证书更新和注销步骤。

[0096] 1.证书更新

[0097] 上一级用户证书更新后,该链条上的下一级用户证书都要更新,即在一个实施例中,上述基于区块链标识的数字证书分级处理方法还可以包括:在检测到根证书、超级节点证书、骨干节点证书和普通节点证书其中的任一级别的证书更新时,更新当前更新证书的下一级证书。具体地,执行检测的操作的主体可以是根证书授权机构节点、超级节点、骨干节点或普通节点,在根证书授权机构节点、超级节点、骨干节点或普通节点检测到根证书、超级节点证书、骨干节点证书和普通节点证书其中的任一级别的证书更新时,可以给当前

节点(例如骨干节点)的下一级别节点发送更新通知,下一级别节点(例如普通节点)更新普通节点证书(当前更新证书的下一级证书)。下面证书过程重新申请及证书注销的执行主体及详细的重新申请注销过程可以参见该证书更新的描述。

[0098] 如用户证书过期了,需要重新申请,上一级用户可重新为其发放证书,即在一个实施例中,上述基于区块链标识的数字证书分级处理方法还可以包括:在检测到根证书、超级节点证书、骨干节点证书和普通节点证书其中的任一级别的证书过期时,向当前过期证书的颁发者重新申请数字证书。

[0099] 2.证书注销

[0100] 用户可自己注销自己的证书;

[0101] 上一级用户证书注销后,该链条上的下一级用户证书都要注销,需要重新申请,即在一个实施例中,上述基于区块链标识的数字证书分级处理方法还可以包括:在检测到上一级用户证书注销后,当前用户证书链条上以下级别用户证书均要注销,需要重新申请。

[0102] 为了便于理解本发明如何实施,下面举两个例子说明基于区块链标识的数字证书分级处理(证书的颁发、验证、更新和注销)的整体过程。

[0103] 示例1:

[0104] 一、证书颁发(根CA内置)。

[0105] 第一步:根CA为超级节点颁发超级节点证书,超级节点证书存储在超级节点上。

[0106] 第二步:超级节点为骨干节点颁发骨干节点证书,骨干节点证书内容和上一个证书的不同:颁发者bid、接受者bid、节点类型、创建者公钥和签名,骨干节点证书存储在骨干节点上。

[0107] 第三步:骨干节点为普通节点颁发普通节点证书,普通节点证书内容和上一个证书的不同:颁发者bid、接受者bid、节点类型、创建者公钥和签名,普通节点证书存储在普通节点上。

[0108] 二、验证证书。

[0109] 第一步:网络根据证书内容找到证书颁发者的公钥和数字签名值,验证其数字签名值,验证通过后,验证是否有上一级证书,如无,验证结束;如有,进行第二步。该案例中普通节点存在上一级节点:骨干节点,故需验证骨干节点证书有效性。

[0110] 第二步:根据骨干节点证书内容找到证书颁发者公钥和数字签名,验证其数字签名值,验证通过后,存在上一级证书节点:超级节点,需验证超级节点证书有效性。

[0111] 第三步:根据超级节点证书内容找到证书颁发者公钥和数字签名,验证其数字签名值,验证通过后验证根CA证书有效性。

[0112] 第四步:根CA证书验证通过后,验证结束。

[0113] 三、证书更新。

[0114] 上一级节点证书更新后,下一级直至末级节点的证书都需要更新,例如,超级节点的证书更新后,该链条上的骨干节点、普通节点的证书都需要更新。

[0115] 四、证书注销。

[0116] 上一级节点证书注销后,下一级直至末级节点的证书都自动注销,例如,超级节点的证书注销后,该链条上的骨干节点、普通节点的证书都被注销。

[0117] 示例2:身份证书的颁发、验证、更新参见上面示例1,和上面的示例1类似,不同的

是证书类型为“身份证书”。

[0118] 综上,本发明实施例提供的基于区块链标识的数字证书分级处理方法的有益技术效果包括:

[0119] 1.采用基于主子链架构的区块链做身份管理,减轻单链负担,提高证书颁发、验证性能。

[0120] 2.采用多级证书验证的方式,在不减少可信度的前提下,减轻根CA负担。

[0121] 3.采用去中心化根CA与中心化系统相结合的方式,中心化系统的根CA在区块链上,减少根CA被篡改的风险。

[0122] 本发明实施例中还提供了一种基于区块链标识的数字证书分级处理装置,如下面的实施例所述。由于该装置解决问题的原理与基于区块链标识的数字证书分级处理方法相似,因此该装置的实施可以参见基于区块链标识的数字证书分级处理方法的实施,重复之处不再赘述。

[0123] 本发明实施例中基于区块链标识的数字证书分级处理装置的结构示意图可以如图4所示,根证书授权机构节点(图4中的CA)和多个超级节点构成主区块链,与每一所述超级节点连接的一个骨干节点和多个普通节点(图4中子链上的“节点”)构成至少一个子区块链,如图4所示,该装置包括:

[0124] 主区块链上的根证书授权机构节点,用于根据根证书为主区块链上的每一超级节点颁发超级节点证书,所述超级节点证书存储在主区块链上;

[0125] 每一超级节点,用于根据所述超级节点证书,为对应的骨干节点颁发骨干节点证书,所述骨干节点证书存储在对应的骨干节点上;

[0126] 每一骨干节点,用于根据所述骨干节点证书,为对应的子区块链上的普通节点颁发普通节点证书,所述普通节点证书存储在子区块链上。

[0127] 在一个实施例中,所述根证书授权机构节点、超级节点、骨干节点或普通节点还可以用于:

[0128] 接收当前数字证书的验证请求;

[0129] 验证所述当前数字证书颁发者的签名;

[0130] 若根据当前数字证书颁发者的签名验证结果,确定当前数字证书存在上一级颁发者时,验证上一级颁发者的签名,直到找到最初的证书颁发者;所述最初的证书颁发者为根证书授权机构节点;

[0131] 如果当前数字证书颁发者到最初的证书颁发者的链条上的数字证书验证均为可信,确定当前数字证书可信。

[0132] 本申请技术方案中对数据的获取、存储、使用、处理等均符合国家法律法规的相关规定。

[0133] 本发明实施例还提供一种计算机设备,包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序,所述处理器执行所述计算机程序时实现上述基于区块链标识的数字证书分级处理方法。

[0134] 本发明实施例还提供一种计算机可读存储介质,所述计算机可读存储介质存储有计算机程序,所述计算机程序被处理器执行时实现上述基于区块链标识的数字证书分级处理方法。

[0135] 本发明实施例还提供一种计算机程序产品,所述计算机程序产品包括计算机程序,所述计算机程序被处理器执行时实现上述基于区块链标识的数字证书分级处理方法。

[0136] 本发明实施例中,基于区块链标识的数字证书分级处理方案,根证书授权机构节点和多个超级节点构成主区块链,与每一所述超级节点连接的一个骨干节点和多个普通节点构成至少一个子区块链,与现有技术中传统数字证书的颁发和验证依赖于中心化的CA机构,身份数据容易被篡改,存在数字证书处理效率和安全性都低的问题的技术方案相比,通过:主区块链上的根证书授权机构节点根据根证书为主区块链上的每一超级节点颁发超级节点证书,所述超级节点证书存储在主区块链上;每一超级节点根据所述超级节点证书,为对应的骨干节点颁发骨干节点证书,所述骨干节点证书存储在对应的骨干节点上;每一骨干节点根据所述骨干节点证书,为对应的子区块链上的普通节点颁发普通节点证书,所述普通节点证书存储在子区块链上,采用基于主子链架构的区块链做数字证书身份处理,可以减轻单链负担,提高证书颁发及后续验证性能,实现了高效安全地分级处理数字证书。

[0137] 本领域内的技术人员应明白,本发明的实施例可提供为方法、系统、或计算机程序产品。因此,本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且,本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0138] 本发明是参照根据本发明实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器,使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0139] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中,使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品,该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0140] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上,使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理,从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0141] 以上所述的具体实施例,对本发明的目的、技术方案和有益效果进行了进一步详细说明,所应理解的是,以上所述仅为本发明的具体实施例而已,并不用于限定本发明的保护范围,凡在本发明的精神和原则之内,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。

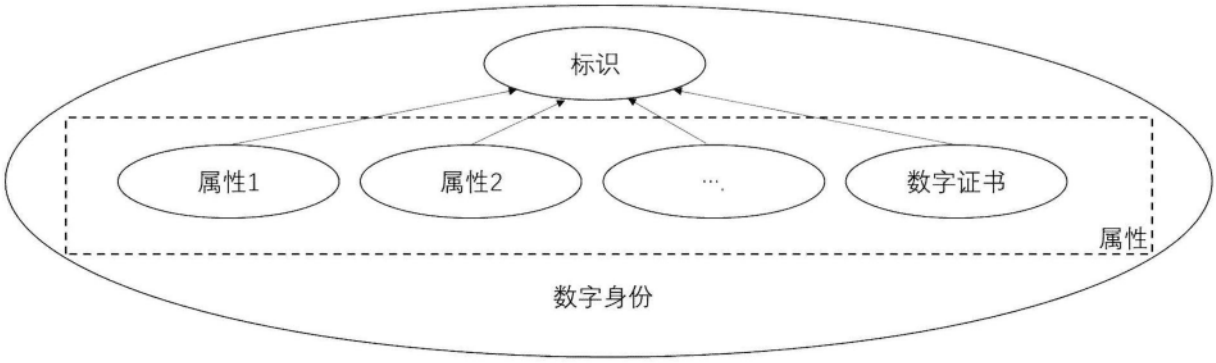

标识
属性1
属性2
....
数字证书
属性
数字身份

图1

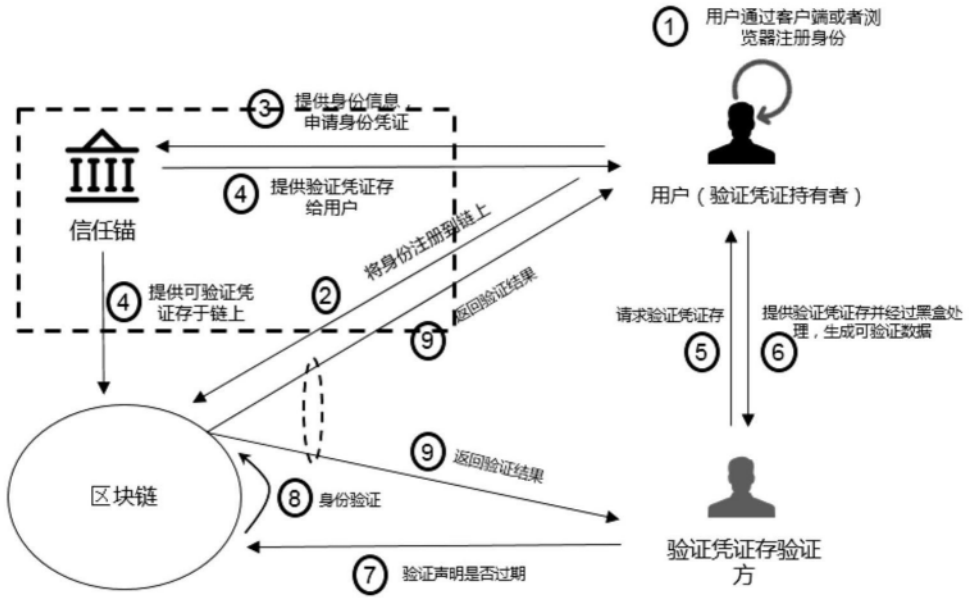

1 用户通过客户端或者浏览器注册身份
3 提供身份信息 申请身份凭证
4 提供验证凭证存给用户
信任锚
用户（验证凭证持有者）
将身份注册到链上
4 提供可验证凭证存于链上
2
返回验证结果
9
请求验证凭证存
5
6 提供验证凭证存并经过黑盒处理，生成可验证数据
9 返回验证结果
区块链
8 身份验证
7 验证声明是否过期
验证凭证存验证方

图2

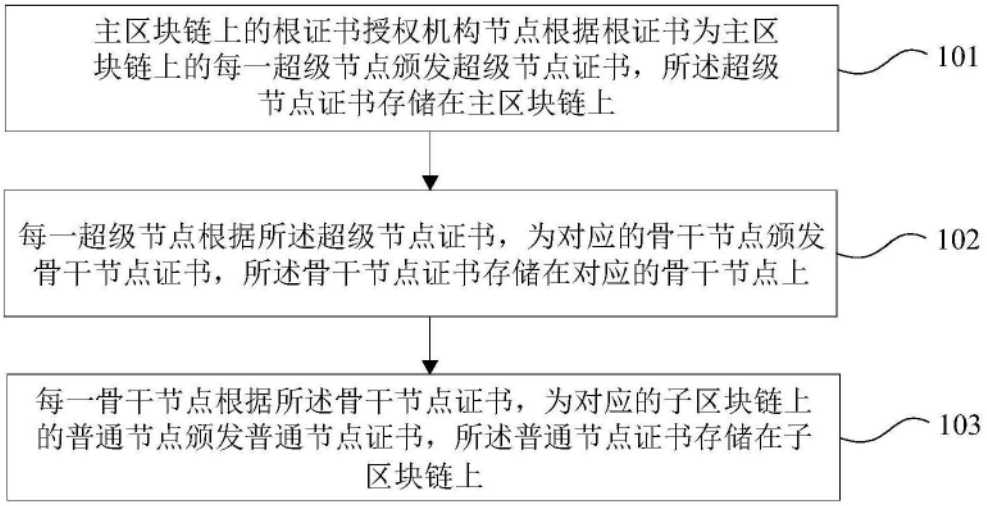

主区块链上的根证书授权机构节点根据根证书为主区块链上的每一超级节点颁发超级节点证书，所述超级节点证书存储在主区块链上
101
每一超级节点根据所述超级节点证书，为对应的骨干节点颁发骨干节点证书，所述骨干节点证书存储在对应的骨干节点上
102
每一骨干节点根据所述骨干节点证书，为对应的子区块链上的普通节点颁发普通节点证书，所述普通节点证书存储在子区块链上
103

图3

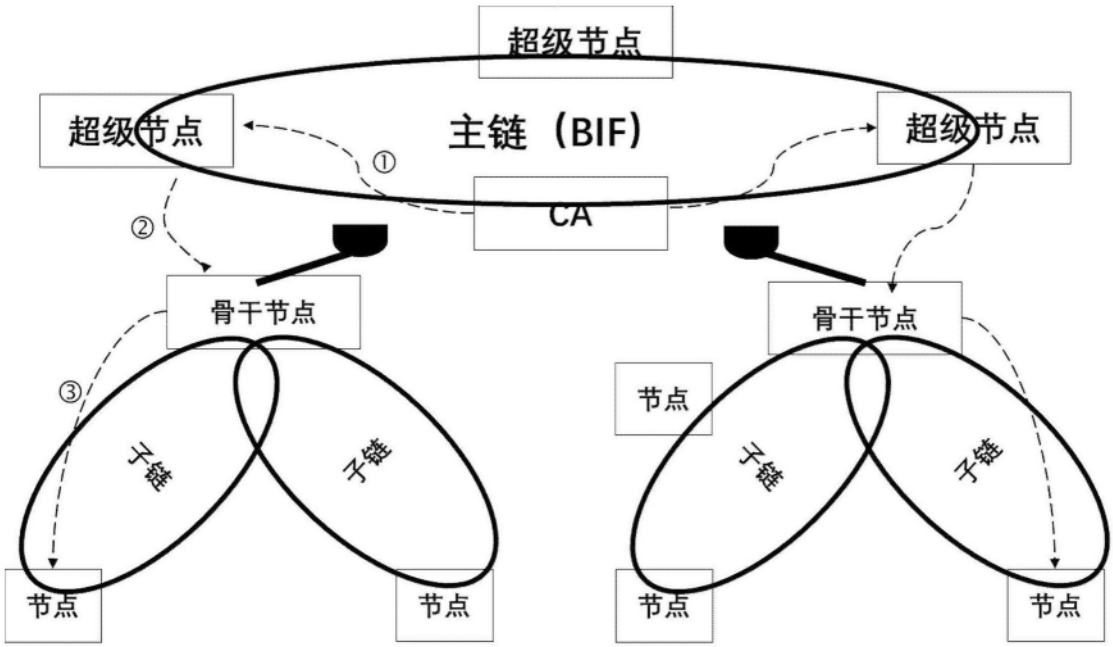

超级节点
超级节点
主链（BIF）
超级节点
①
CA
②
骨干节点
骨干节点
③
子链
子链
节点
节点
节点
子链
子链
节点

图4

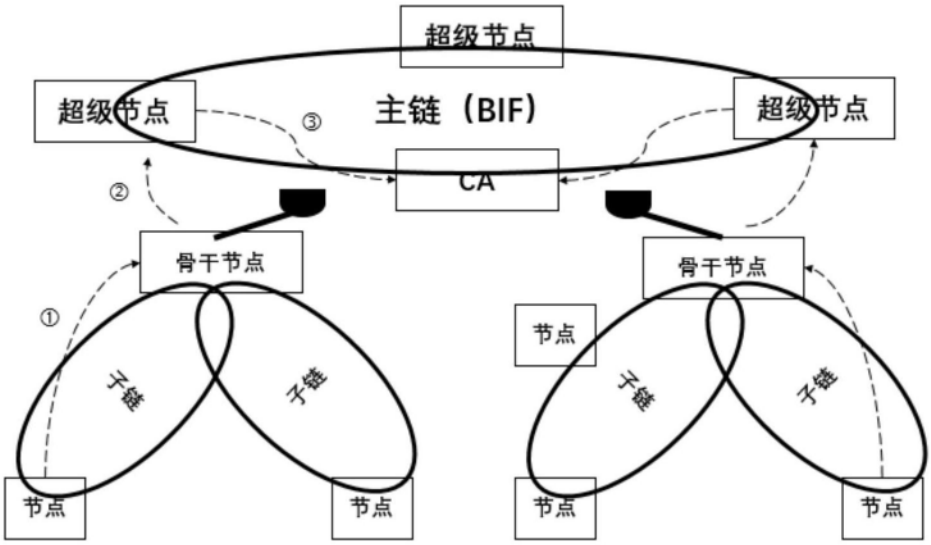


图5

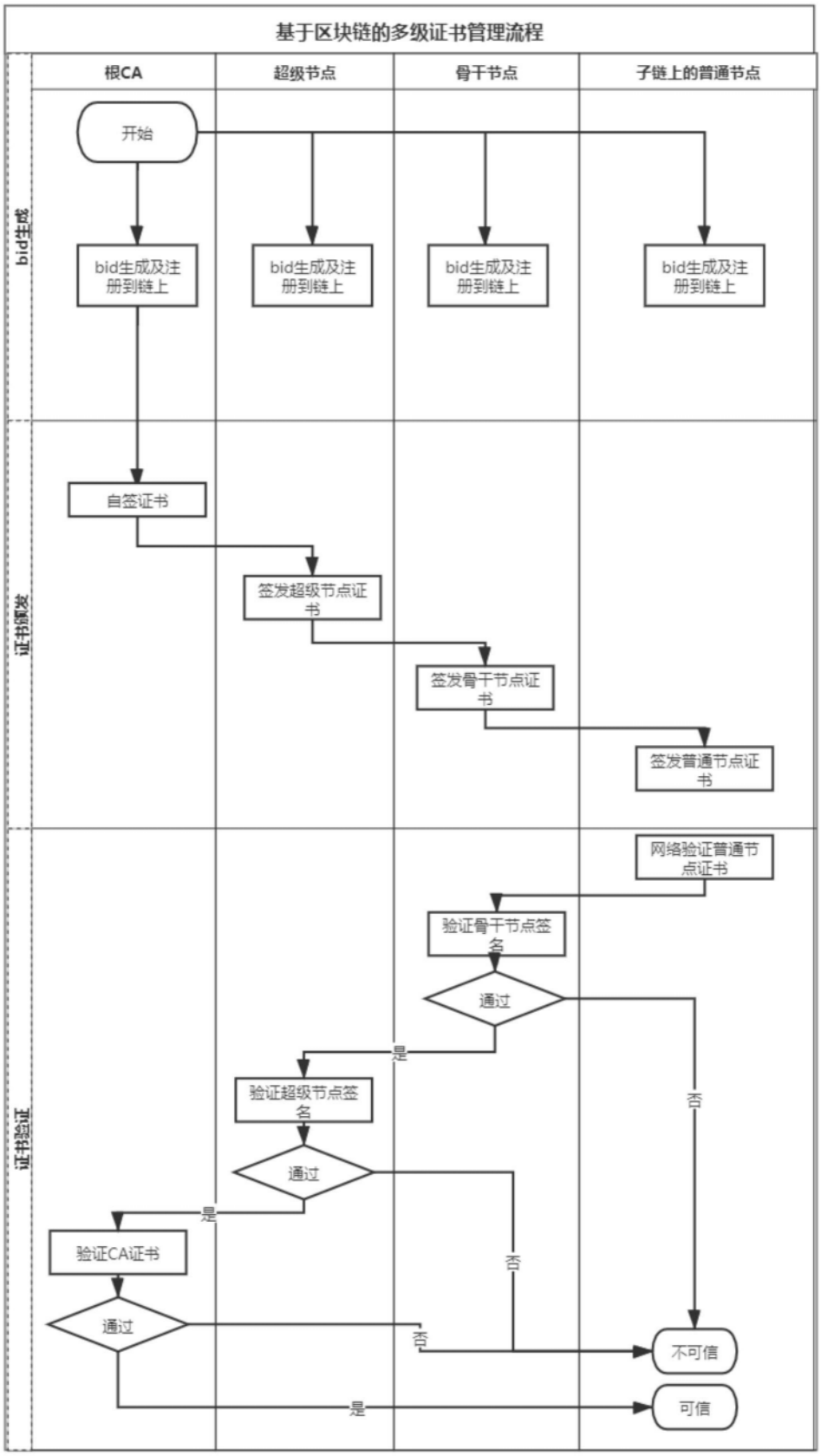

基于区块链的多级证书管理流程
根CA
超级节点
骨干节点
子链上的普通节点
bid生成
证书颁发
证书验证
开始
bid生成及注册到链上
bid生成及注册到链上
bid生成及注册到链上
bid生成及注册到链上
自签证书
签发超级节点证书
签发骨干节点证书
签发普通节点证书
网络验证普通节点证书
验证骨干节点签名
通过
是
否
验证超级节点签名
通过
是
否
验证CA证书
通过
否
是
不可信
可信

图6

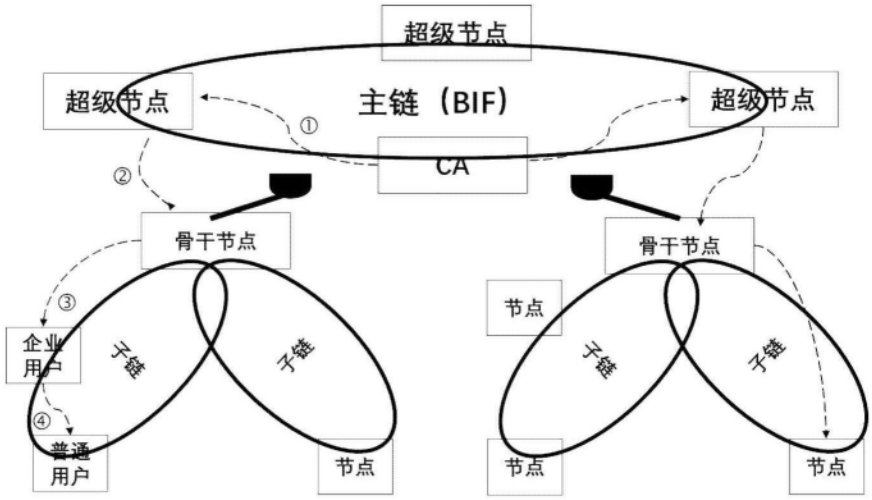

超级节点
超级节点
主链（BIF）
超级节点
①
CA
②
骨干节点
骨干节点
③
企业用户
子链
子链
节点
子链
子链
④
普通用户
节点
节点
节点

图7

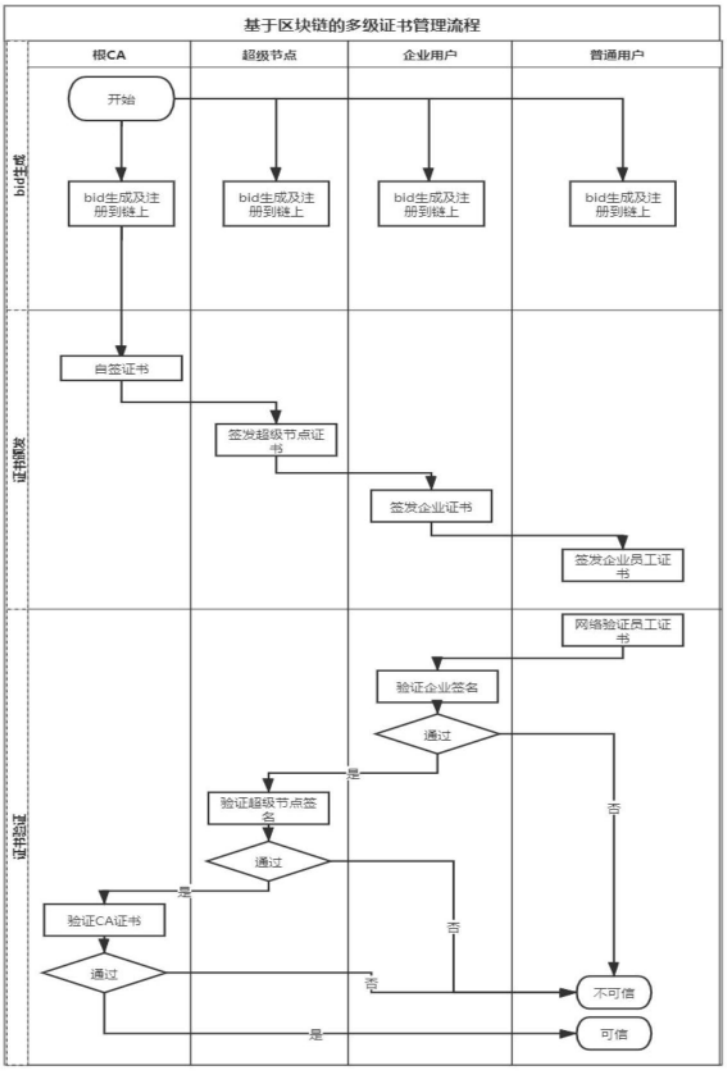

基于区块链的多级证书管理流程
根CA
超级节点
企业用户
普通用户
bid书城
证书颁发
证书验证
开始
bid生成及注册到链上
bid生成及注册到链上
bid生成及注册到链上
bid生成及注册到链上
自签证书
签发超级节点证书
签发企业证书
签发企业员工证书
网络验证员工证书
验证企业签名
通过
是
否
验证超级节点签名
通过
是
否
验证CA证书
通过
否
是
不可信
可信

图8