(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 111832004 B
(45)授权公告日 2024.05.17

(21)申请号 202010620574.4

(22)申请日 2020.06.30

(65)同一申请的已公布的文献号
申请公布号 CN 111832004 A

(43)申请公布日 2020.10.27

(73)专利权人 北京泰尔英福科技有限公司
地址 101300 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 金键 曾西平 张发振 胡键伟 史维君 李慧玲 郭健 单鹏飞 阚雪娇 周厚发 王颜飞

(74)专利代理机构 北京路浩知识产权代理有限公司 11002
专利代理师 李文清

(51)Int.Cl.
G06F 21/44(2013.01)

(56)对比文件
CN 105591753 A,2016.05.18
CN 105592098 A,2016.05.18
CN 108052530 A,2018.05.18
CN 108389045 A,2018.08.10
CN 108512667 A,2018.09.07
CN 109150539 A,2019.01.04
CN 111049658 A,2020.04.21
CN 111277577 A,2020.06.12
US 2009072032 A1,2009.03.19
US 2017109955 A1,2017.04.20
US 2017330174 A1,2017.11.16
US 2020162261 A1,2020.05.21
W. -T. Tsai.“Design Issues in Permissioned Blockchains for Trusted Computing”.2017 IEEE Symposium on Service-Oriented System Engineering.2017,153-159.
周云.基于区块链的信息网络信任支撑环境构建研究.信息安全与通信保密.2020,(第04期),82-90.
任彦冰;李兴华;刘海;程庆丰;马建峰.基于区块链的分布式物联网信任管理方法研究.计算机研究与发展.2018,(第07期),1462-1478.
胡键伟;尹丰.去中心化应用(DApp)技术原理和质量评测分析.中国新通信.2018,(第17期),100-100.

审查员 唐季超

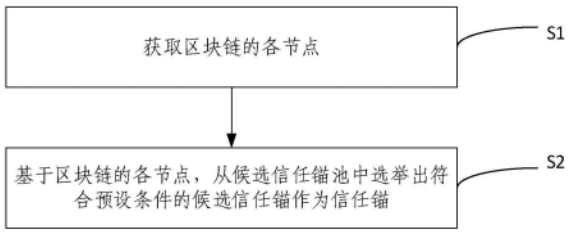
权利要求书2页 说明书10页 附图1页

(54)发明名称

可信声明系统中信任锚的管理方法及装置

(57)摘要

本发明实施例提供了一种可信声明系统中信任锚的管理方法及装置,通过区块链的各节点实现对候选信任锚的去中心化选举,得到最终可用的信任锚,对信任锚的产生进行管理。通过选举的方式为普通用户/企业提供了成为信任锚的途径,使可信声明系统中的信任锚颁布的可信声明的可信性提高,不受可信声明运营商主导,为签发多维度可信声明提供了便利。



CN 111832004 B

1.一种可信声明系统中信任锚的管理方法,其特征在于,包括:

基于区块链的各节点,从候选信任锚池中选举出符合预设条件的候选信任锚作为信任锚;

其中,所述预设条件包括所述候选信任锚在选举过程中得到的权益分排序在前第一预设数量内,或者所述候选信任锚在选举过程中得到的票数在前第二预设数量内,或者所述候选信任锚在选举过程中得到的信用分在前第三预设数量内;

还包括:

基于预设更新条件,对所述候选信任锚池进行更新;

其中,所述预设更新条件包括预设更新周期和/或预设更新需求;

所述候选信任锚具体包括多种不同类别的候选信任锚,每种类别的候选信任锚对应一预设更新周期;相应地,所述基于预设更新条件,对所述候选信任锚池进行更新,具体包括:

基于每种类别的候选信任锚对应的预设更新周期,对所述候选信任锚池中每种类别的候选信任锚进行更新;

所述基于区块链的各节点,从候选信任锚池中选举出符合预设条件的候选信任锚作为信任锚,具体包括:

将所述区块链的超级节点和/或普通用户节点作为投票者,对所述候选信任锚池中的每个候选信任锚进行投票,从候选信任锚池中选举出符合预设条件的候选信任锚作为信任锚;

每个投票者均携带有权益分以及信用分,所述候选信任锚在选举过程中得到的权益分为对所述候选信任锚进行投票的所有投票者携带的权益分之和,所述候选信任锚在选举过程中得到的信用分为对所述候选信任锚进行投票的所有投票者携带的信用分之和;

所述预设更新需求是信任锚颁发的证书即将过期时发起候选信任锚池更新事件,或者有新用户申请成为候选信任锚;

各投票者携带的信用分具体的计算规则如下:

信任分=(使用率*80%+投诉率*20%)*100;

投诉率=1-信任锚投诉个数/信任锚最大投诉个数;

使用率=信任锚颁发证书个数/信任锚颁发最大证书个数;

所述信任锚的类别包括基础信任锚,对于所述基础信任锚,每颁发一份可信凭证获得相应的积分奖励,所述积分奖励按照服务的稳定性以及投诉占比决定。

2.根据权利要求1所述的可信声明系统中信任锚的管理方法,其特征在于,所述信任锚的类别包括基础信任锚和扩展信任锚;

所述基础信任锚的投票者为所述超级节点,所述扩展信任锚的投票者为所述普通用户节点;或者,所述基础信任锚以及所述扩展信任锚的投票者均为所述超级节点;或者,所述基础信任锚以及所述扩展信任锚的投票者均为所述普通用户节点。

3.根据权利要求1-2中任一项所述的可信声明系统中信任锚的管理方法,其特征在于,还包括:

对所述信任锚进行服务信息修改、服务连接的连通测试、撤销申请的审批以及用户投诉的审批。

4.一种可信声明系统中信任锚的管理装置,其特征在于,包括:

选举模块,用于基于区块链的各节点,从候选信任锚池中选举出符合预设条件的候选信任锚作为信任锚;

其中,所述预设条件包括所述候选信任锚在选举过程中得到的权益分排序在前第一预设数量内,或者所述候选信任锚在选举过程中得到的票数在前第二预设数量内,或者所述候选信任锚在选举过程中得到的信用分在前第三预设数量内;

还包括:更新模块,所述更新模块用于:

将所述信任锚添加至信任锚池;

基于预设更新条件,对所述信任锚池进行更新;

其中,所述预设更新条件包括预设更新周期和/或预设更新需求;

所述候选信任锚具体包括多种不同类别的候选信任锚,每种类别的候选信任锚对应一预设更新周期;相应地,所述更新模块具体用于:

基于每种类别的候选信任锚对应的预设更新周期,对所述候选信任锚池中每种类别的候选信任锚进行更新;

所述选举模块,具体用于:

将所述区块链的超级节点和/或普通用户节点作为投票者,对所述候选信任锚池中的每个候选信任锚进行投票,从候选信任锚池中选举出符合预设条件的候选信任锚作为信任锚;

每个投票者均携带有权益分以及信用分,所述候选信任锚在选举过程中得到的权益分为对所述候选信任锚进行投票的所有投票者携带的权益分之和,所述候选信任锚在选举过程中得到的信用分为对所述候选信任锚进行投票的所有投票者携带的信用分之和;

所述预设更新需求是信任锚颁发的证书即将过期时发起候选信任锚池更新事件,或者有新用户申请成为候选信任锚;

各投票者携带的信用分具体的计算规则如下:

信任分=(使用率*80%+投诉率*20%)*100;

投诉率=1-信任锚投诉个数/信任锚最大投诉个数;

使用率=信任锚颁发证书个数/信任锚颁发最大证书个数;

所述信任锚的类别包括基础信任锚,对于所述基础信任锚,每颁发一份可信凭证获得相应的积分奖励,所述积分奖励按照服务的稳定性以及投诉占比决定。

5.一种电子设备,包括:存储器、处理器以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程序时实现如权利要求1-3中任一项所述的可信声明系统中信任锚的管理方法的步骤。

6.一种非暂态计算机可读存储介质,其上存储有计算机程序,其特征在于,该计算机程序被处理器执行时实现如权利要求1-3中任一项所述的可信声明系统中信任锚的管理方法的步骤。

可信声明系统中信任锚的管理方法及装置

技术领域

[0001] 本发明涉及计算机技术领域,更具体地,涉及可信声明系统中信任锚的管理方法及装置。

背景技术

[0002] 信任锚即信任的起点,是指在信任模型中能够证明某一实体身份的身份签发者。经信任锚证明后的实体身份为可信身份。

[0003] 目前,基于区块链的可信声明系统中的信任锚,大多由可信声明运营方预置在可信声明系统中,用户无法参与信任锚的产生过程。由于可信声明系统内的信任锚是预置的,管理比较集中,没有给普通用户/企业提供成为信任锚的途径,这样信任锚颁布的可信声明的可信性也会由可信声明运营商主导,会存在过分依赖可信声明运营商的问题,一方面,对签发多维度可信声明产生限制,另一方面,用户会对信任锚颁发的可信声明的可信性产生怀疑。

[0004] 因此,现急需提供一种可信声明系统中信任锚的管理方法及装置。

发明内容

[0005] 为克服上述问题或者至少部分地解决上述问题,本发明实施例提供了一种可信声明系统中信任锚的管理方法及装置。

[0006] 第一方面,本发明实施例提供了一种可信声明系统中信任锚的管理方法,包括:

[0007] 基于区块链的各节点,从候选信任锚池中选举出符合预设条件的候选信任锚作为信任锚;

[0008] 其中,所述预设条件包括所述候选信任锚在选举过程中得到的权益分排序在前第一预设数量内,或者所述候选信任锚在选举过程中得到的票数在前第二预设数量内,或者所述候选信任锚在选举过程中得到的信用分在前第三预设数量内。

[0009] 优选地,所述的可信声明系统中信任锚的管理方法,还包括:

[0010] 基于预设更新条件,对所述候选信任锚池进行更新;

[0011] 其中,所述预设更新条件包括预设更新周期和/或预设更新需求。

[0012] 优选地,所述候选信任锚具体包括多种不同类别的候选信任锚,每种类别的候选信任锚对应一预设更新周期;相应地,所述基于预设更新条件,对所述候选信任锚池进行更新,具体包括:

[0013] 基于每种类别的候选信任锚对应的预设更新周期,对所述候选信任锚池中每种类别的候选信任锚进行更新。

[0014] 优选地,所述基于区块链的各节点,从候选信任锚池中选举出符合预设条件的候选信任锚作为信任锚,具体包括:

[0015] 将所述区块链的超级节点和/或普通用户节点作为投票者,对所述候选信任锚池中的每个候选信任锚进行投票,从候选信任锚池中选举出符合预设条件的候选信任锚作为

信任锚；

[0016] 每个投票者均携带有权益分以及信用分，所述候选信任锚在选举过程中得到的权益分为对所述候选信任锚进行投票的所有投票者携带的权益分之和，所述候选信任锚在选举过程中得到的信用分为对所述候选信任锚进行投票的所有投票者携带的信用分之和。

[0017] 优选地，所述信任锚的类别包括基础信任锚和扩展信任锚；

[0018] 所述基础信任锚的投票者为所述超级节点，所述扩展信任锚的投票者为所述普通用户节点；或者，所述基础信任锚以及所述扩展信任锚的投票者均为所述超级节点；或者，所述基础信任锚以及所述扩展信任锚的投票者均为所述普通用户节点。

[0019] 优选地，所述的可信声明系统中信任锚的管理方法，还包括：

[0020] 对所述信任锚进行服务信息修改、服务连接的连通测试、撤销申请的审批以及用户投诉的审批。

[0021] 第二方面，本发明实施例提供了一种可信声明系统中信任锚的管理装置，包括：选举模块。其中，

[0022] 选举模块用于基于区块链的各节点，从候选信任锚池中选举出符合预设条件的候选信任锚作为信任锚；

[0023] 其中，所述预设条件包括所述候选信任锚在选举过程中得到的权益分排序在前第一预设数量内，或者所述候选信任锚在选举过程中得到的票数在前第二预设数量内，或者所述候选信任锚在选举过程中得到的信用分在前第三预设数量内。

[0024] 优选地，可信声明系统中信任锚的管理装置，还包括：更新模块，所述更新模块用于：

[0025] 将所述信任锚添加至信任锚池；

[0026] 基于预设更新条件，对所述信任锚池进行更新；

[0027] 其中，所述预设更新条件包括预设更新周期和/或预设更新需求。

[0028] 第三方面，本发明实施例提供了一种电子设备，包括：存储器、处理器以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程序时实现如第一方面所述的可信声明系统中信任锚的管理方法的步骤。

[0029] 第四方面，本发明实施例提供了一种非暂态计算机可读存储介质，其上存储有计算机程序，该计算机程序被处理器执行时实现如第一方面所述的可信声明系统中信任锚的管理方法的步骤。

[0030] 本发明实施例提供的一种可信声明系统中信任锚的管理方法及装置，通过区块链的各节点实现对候选信任锚的去中心化选举，得到最终可用的信任锚，对信任锚的产生进行管理。通过选举的方式为普通用户/企业提供了成为信任锚的途径，使可信声明系统中的信任锚颁布的可信声明的可信性提高，不受可信声明运营商主导，为签发多维度可信声明提供了便利。

附图说明

[0031] 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一简单地介绍，显而易见地，下面描述中的附图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。

[0032] 图1为本发明实施例提供的一种可信声明系统中信任锚的管理方法的流程示意图;

[0033] 图2为本发明实施例提供的一种可信声明系统中信任锚的管理装置的结构示意图;

[0034] 图3为本发明实施例提供的一种电子设备的结构示意图。

具体实施方式

[0035] 为使本发明实施例的目的、技术方案和优点更加清楚,下面将结合本发明实施例中的附图,对本发明实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例是本发明一部分实施例,而不是全部的实施例。基于本发明中的实施例,本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例,都属于本发明保护的范围。

[0036] 目前,信任锚的产生方式通常是由可信声明运营商在可信声明系统中内置,即实现中心化部署,内置的信任锚不需要选举,信任锚的更新由可信声明运营商决定。例如,发证方用户申请(Claim)成为信任锚时,需要知道发证方用户相关信息,包括发证方用户申请(Claim)服务的端点(Endpoint)等,这类信息会由发证方用户公布在自己的主页上。同时,提供声明发行注册(Claim Issuer Registry)服务,即发证方用户注册时,用来对外发布一些已知的发证方用户列表及其相关信息。由于可信声明系统内的信任锚是预置的,管理比较集中,没有给普通用户/企业提供成为信任锚的途径,这样信任锚颁布的可信声明的可信性也会由可信声明运营商主导,会存在过分依赖可信声明运营商的问题,一方面,对签发多维度可信声明产生限制,另一方面,用户会对信任锚颁发的可信声明的可信性产生怀疑。基于此,本发明实施例中提供了一种可信声明系统中信任锚的管理方法。

[0037] 如图1所示,本发明实施例提供了一种可信声明系统中信任锚的管理方法,包括:

[0038] S1,获取区块链的各节点;

[0039] S2,基于区块链的各节点,从候选信任锚池中选举出符合预设条件的候选信任锚作为信任锚;

[0040] 其中,所述预设条件包括所述候选信任锚在选举过程中得到的权益分排序在前第一预设数量内,或者所述候选信任锚在选举过程中得到的票数在前第二预设数量内,或者所述候选信任锚在选举过程中得到的信用分在前第三预设数量内。

[0041] 具体地,本发明实施例中提供的可信声明系统中信任锚的管理方法,其执行主体为可信声明系统。可信声明系统依托于区块链实现对信任锚的管理。可信声明系统又可以称为可信系统、可验证声明系统等。信任锚是指可信的身份签发者,也可以称为信任根、证书签发者、发证方、信任源、可信身份的签发/发行者、可验证声明的签发者/发行者等。对信任锚的管理,可以包括信任锚的产生、更新、信息的修改、服务连接的连通测试、撤销申请的审批以及用户投诉的审批等操作。

[0042] 首先,执行步骤S1。区块链的节点可以包括超级节点和普通用户节点,超级节点具有记账、选举以及竞选等功能,普通用户节点不包括记账的超级节点,具有选举功能。

[0043] 然后,执行步骤S2。通过区块链的各节点,对候选信任锚池中的候选信任锚进行选举,以选出可用的信任锚,即符合预设条件的候选信任锚。候选信任锚池中存储有多个候选

信任锚,候选信任锚是区块链上可以进行证书颁发的发证方用户,发证方用户向可信声明系统申请成为信任锚时,先需要进行审核,审核通过成为候选信任锚。候选信任锚和信任锚的种类均可以包括身份信任锚、学历信任锚、不良信息验证信任锚等,分别对应于进行身份验证、学历验证、不良信息验证等证书颁发的发证方用户。每种候选信任锚的数量可以根据需要进行设定,本发明实施例中对此不作具体限定。

[0044] 本发明实施例中,信任锚的产生由区块链的各节点对候选信任锚进行去中心化选举得到,即区块链的各节点作为投票方,从发证方用户申请成为信任锚得到的候选信任锚池中,选举出一定数量、一定种类可用的信任锚。数量个数和种类个数可以由候选信任锚的种类确定,如有K类发证方用户申请成为信任锚,且均通过审核,则有K类候选信任锚,从中可以确定J类信任锚,J≤K(J=1,2,3…,K=1,2,3…)。如确定了J类信任锚,则可以进一步从每种信任锚中选定L个信任锚(L=1,2,3…)。

[0045] 需要说明的是,本发明实施例中,候选信任锚成为信任锚需要满足的预设条件是候选信任锚在选举过程中得到的权益分排序在前第一预设数量内,或者候选信任锚在选举过程中得到的票数在前第二预设数量内,或者候选信任锚在选举过程中得到的信用分在前第三预设数量内。候选信任锚在选举过程中得到的权益分以及信用分分别是为该候选信任锚投票的投票方的权益分以及信用分之和,得到的票数是该候选信任锚获得的票数,若每个投票方只能给同一个候选信任锚投票一次,则得到的票数也等于为该候选信任锚投票的投票方的数量。第一预设数量、第二预设数量以及第三预设数量均可以根据需要进行设定,例如第一预设数量取值为M(M=1,2,3,…),则需要从候选信任锚池中选举出权益分排序在前的M个候选信任锚作为信任锚,即有M个信任锚。第二预设数量取值为N(N=1,2,3,…),则需要从候选信任锚池中选举出票数排序在前的N个候选信任锚作为信任锚,即有N个信任锚。第三预设数量取值为O(O=1,2,3,…),则需要从候选信任锚池中选举出信用分排序在前的O个候选信任锚作为信任锚,即有O个信任锚。

[0046] 本发明实施例中提供的可信声明系统中信任锚的管理方法,通过区块链的各节点实现对候选信任锚的去中心化选举,得到最终可用的信任锚,对信任锚的产生进行管理。通过选举的方式为普通用户/企业提供了成为信任锚的途径,使可信声明系统中的信任锚颁布的可信声明的可信性提高,不受可信声明运营商主导,为签发多维度可信声明提供了便利。

[0047] 在上述实施例的基础上,本发明实施例中可以在去中心化选举的基础上,结合可信声明系统内置的信任锚共同得到信任锚。内置的信任锚由数字身份分发商决定,如某类信任锚过期,可信声明系统将续期、更换或删除该信任锚。可信声明系统内置一定数量、一定种类的信任锚,例如针对身份验证、学历验证、不良信息验证等分别内置身份信任锚、学历信任锚和不良信息验证信任锚。信任锚种类根据主要验证的可信声明的属性划分;种类的个数和每类信任锚的数量由数字身份分发商确定,内置的数量可以为每类一个,也可以为每类多个,本发明实施例中对此不作具体限定。

[0048] 如果选用按投票方的数字身份计票的方式选举信任锚,则需要用户通过身份验证,才能进行后续的申请成为信任锚操作或者投票选举信任锚操作。内置的信任锚公信度较高,为用户完成重要基本属性的验证,如身份属性(具体属性根据数字身份提供的主要服务决定)验证。完成数字身份验证的用户即成为候选信任锚,可以进一步申请成为信任锚。

需要说明的是,每个数字身份只能投一票,即如一个用户有多个区块链标识,通过身份验证后为同一个用户,则多个标识在一次选举中只能投票一次;一个数字身份可以给多个候选信任锚投票。

[0049] 在上述实施例的基础上,本发明实施例中提供了一种可信声明系统中信任锚的管理方法,还包括:

[0050] 基于预设更新条件,对所述候选信任锚池进行更新;

[0051] 其中,所述预设更新条件包括预设更新周期和/或预设更新需求。

[0052] 具体地,本发明实施例中,可以根据预设更新条件对候选信任锚池进行更新。预设更新条件可以是预设更新周期或者预设更新需求,或者预设更新周期以及预设更新需求的结合。对候选信任锚池的更新是指改变候选信任锚池内的组成,即改变候选信任锚池内包含的候选信任锚及其数量。例如,候选信任锚池内包含有候选信任锚a、b、c、d,则更新后的候选信任锚池内可以增加候选信任锚e,也可以将候选信任锚a替换为候选信任锚e。

[0053] 预设更新周期可以根据需要进行设定,候选信任锚池中的所有种类的候选信任锚按照相同的预设更新周期T_1更新(T_1=1,2,3,…天),例如T_1=1个月,即每隔1个月对候选信任锚池进行更新。预设更新需求可以是信任锚颁发的证书即将过期时,发起候选信任锚池更新事件;用户响应候选信任锚池更新事件申请成为信任锚,通过审核后,候选信任锚池完成更新。预设更新需求还可以是有新用户申请成为候选信任锚;该用户通过审核后,候选信任锚池完成更新。

[0054] 在上述实施例的基础上,本发明实施例中提供了一种可信声明系统中信任锚的管理方法,所述候选信任锚具体包括多种不同类别的候选信任锚,每种类别的候选信任锚对应一预设更新周期;相应地,所述基于预设更新条件,对所述候选信任锚池进行更新,具体包括:

[0055] 基于每种类别的候选信任锚对应的预设更新周期,对所述候选信任锚池中每种类别的候选信任锚进行更新。

[0056] 具体地,本发明实施例中,为候选信任锚池内不同类别的候选信任锚分别设置预设更新周期,例如,身份验证候选信任锚和学历验证候选信任锚的更新周期较长,设置为1年,社交平台候选信任锚的更新周期较短,设置为3个月。

[0057] 在上述实施例的基础上,还可以对候选信任锚池内的候选信任锚进行更新,具体可以是当候选信任锚池有更新时,即发起候选信任锚更新;还可以是当候选信任锚池中某一类候选信任锚即将过期时,发起候选信任锚更新。

[0058] 在上述实施例的基础上,本发明实施例中提供了一种可信声明系统中信任锚的管理方法,所述基于区块链的各节点,从候选信任锚池中选举出符合预设条件的候选信任锚作为信任锚,具体包括:

[0059] 将所述区块链的超级节点和/或普通用户节点作为投票者,对所述候选信任锚池中的每个候选信任锚进行投票,从候选信任锚池中选举出符合预设条件的候选信任锚作为信任锚;

[0060] 每个投票者均携带有权益分以及信用分,所述候选信任锚在选举过程中得到的权益分为对所述候选信任锚进行投票的所有投票者携带的权益分之和,所述候选信任锚在选举过程中得到的信用分为对所述候选信任锚进行投票的所有投票者携带的信用分之和。

[0061] 具体地,本发明实施例中,区块链的各节点包括超级节点和普通用户节点,二者都可以作为投票者对候选信任锚进行投票,选举出信任锚。当投票由超级节点执行时,超级节点既有记账功能,也有信任锚的选举功能;超级节点同时记账和竞选信任锚时,该超级节点没有选举权。超级节点具体采用DPoS机制实现选举。当投票由普通用户节点执行时,普通用户节点不包括记账的超级节点,且拥有数字身份的普通用户节点都可以成为投票候选人,从中选取N个作为投票者。N个投票者的选取方式可以是随机选取,也可以是选取信用分大于预设阈值的普通用户节点。

[0062] 超级节点和/或普通用户节点共同构成的投票者的数量可以根据经验值设定,也可以设置一比例系数v,在符合要求的指定数量k的投票者中选择v×k个投票者。比例系数v可以根据经验值进行设定。

[0063] 若投票方是用DPoS选出来的,则预设条件由候选信任锚的权益分决定,设候选信任锚j,为候选信任锚j投票的用户i的权益分为q_i,总共投票的用户为B个,则候选信任锚j得到的权益分为$\sum_{i=1}^{B} q_i$。将每类候选信任锚得到的权益分排序,选取前n个作为该类中的信任锚;预设条件还可以由候选信任锚得到的票数决定,将每类每个候选信任锚得到的票数排序,选取前n个作为该类中的信任锚;预设条件还可以由候选信任锚得到的信用分决定,为候选信任锚j投票的用户i的信用分为p_i,总共投票的用户为C个,则候选信任锚j得到的信用分为$\sum_{i=1}^{C} p_i$。将每类候选信任锚得到的信用分排序,选取前n个作为该类中的信任锚。

[0064] 在上述实施例的基础上,本发明实施例中提供了一种可信声明系统中信任锚的管理方法,所述信任锚的类别包括基础信任锚和扩展信任锚;

[0065] 所述基础信任锚的投票者为所述超级节点,所述扩展信任锚的投票者为所述普通用户节点;或者,所述基础信任锚以及所述扩展信任锚的投票者均为所述超级节点;或者,所述基础信任锚以及所述扩展信任锚的投票者均为所述普通用户节点。

[0066] 具体地,本发明实施例中,在可信声明系统中信任锚主要分为基础信任锚以及扩展信任锚。以下仅以基础信任锚的投票者为超级节点,扩展信任锚的投票者为普通用户节点为例进行说明。基础信任锚由超级节点投票产生,此时基础信任锚为中心化信任锚,该信任锚只能由超级节点注册管理等。扩展信任锚由用户可随意注册产生。

[0067] 基础信任锚通过超级节点产生时,只有超级节点有资格注册并选举基础信任锚,用户在注册成为信任锚时需要抵押1000积分,以防止信任锚作恶或者随意退出。具体来说,某一个用户要注册自己为基础信任锚,必须先提交申请并填写信任锚相关的资料(该功能在官网实现),然后由超级节点用户审核资料(审核流程再定),如果通过审核,则由超级节点添加该信任锚信息到链上进入候选列表,最后当信任锚获得3分之2的超级节点投票,则成为可用的信任锚。

[0068] 需要说明的是,基础信任锚的申请实体必须为公司或者组织,因此在审核材料的过程中要对实体资质进行审核。

[0069] 扩展信任锚是指用户可以根据自己提供的服务直接注册成为的信任锚,不需要通过选举机制,不过用户在注册成为信任锚时需要抵押100积分,以防止信任锚作恶或者随意退出。

[0070] 对于扩展信任锚而言,为了鼓励信任锚提供更好的服务以及方便平台筛选中用户更需要更好的信任锚,因此平台会根据信任锚颁发的证书个数以及投诉占比为每个信任锚打信用分,信用分会直接影响信任锚颁发证书获得积分数量并且在投票代理中也会有相应的展现(比如对于扩展信任锚而言会根据信任锚信用分进行排名,信用分越高将排在越前面),信任锚的初始信任分为零。

[0071] 信用分具体的计算规则如下(信用分会每日更新):

[0072] 信任分=(使用率*80%+投诉率*20%)*100;

[0073] 投诉率=1-信任锚投诉个数/信任锚最大投诉个数;

[0074] 使用率=信任锚颁发证书个数/信任锚颁发最大证书个数。

[0075] 在上述实施例的基础上,本发明实施例中提供了一种可信声明系统中信任锚的管理方法,还包括:

[0076] 对所述信任锚进行服务信息修改、服务连接的连通测试、撤销申请的审批以及用户投诉的审批。

[0077] 具体地,本发明实施例中,信任锚具有基础信息以及服务信息,基础信息可以由信任锚自行修改。服务信息包括服务连接信息,在对服务信息进行修改时,必须提交申请最后由超级节点审核并在审核通过后做相应的更新。

[0078] 服务连接的连通测试是指对信任锚服务的周期性检查工作,在区块链上每天固定时间对所有的信任锚提供的服务连接进行连通测试,如果连续三次服务无法接通的话,该信任锚状态自动调为待恢复状态。之后每隔一天检查一次,如果连续一周(该时间为累计时间即包含前三天)服务任然没有连通,则将该信任锚踢出。信任锚被踢出之后,需要同步完成以下两件事:由该信任锚颁发的证书将全部失效,用户需要重新选择信任的信任锚进行认证。该信任锚将减掉之前所获得积分或者币的30%并且扣除所有抵押积分,作为惩罚。

[0079] 撤销申请的审批是指如果信任锚不提供服务了,需要提前一周提出申请,在这一周时间内该信任锚的状态改为暂停提供服务状态,并提供相应的解释以便用户及时去使用其他信任锚提供的服务以便不应该正常使用。当信任锚提出删除服务后,将不再对外提供服务,并且对该信任锚也不进行周期性监测。等一周时间过后系统自动删除信任锚并归还抵押积分。

[0080] 用户投诉的审批是指当用户使用该信任锚时,由于信任锚提供的服务不稳定或者颁发的证书存在错误时,可以对信任锚提出投诉并且该投诉会自动发送到信任锚服务邮箱中以便作出及时的调整,用户只能对已经使用过的信任锚进行投诉并且该投诉为“实名投诉“即每个实体只能投诉一次。用户的投诉会影响信任锚获得的激励积分。当信任锚的投诉占比超过50%时,系统将扣除信任锚抵押积分,并且暂停服务,只有信任锚补交抵押金后才可以继续颁发证书,可信声明系统将在每季度统计一次并作出相应的处理。

[0081] 在上述实施例的基础上,候选信任锚池内的候选信任锚还可以自行撤销退出候选信任锚池,可信声明系统将自动退还抵押积分。

[0082] 在上述实施例的基础上,可信声明系统还可以引入激励措施使用户积极申请成为信任锚。激励措施具体为:

[0083] 对于基础信任锚而言每颁发一份可信凭证将获得相应的积分奖励,该奖励按照服务的稳定性以及投诉占比决定。对于基础信任锚而言前期每颁发一份凭证将获得2个积分

作为奖励,之后在信任锚加入的前三年内每半年根据提供的服务以及投诉占比做相应的调整,满三年后每年调整一次。具体调整规则如下:

[0084] 根据稳定性调整(按天作为标准),天数不能叠加(即每次调整完后,数据清空重新开始计数)

[0085] 稳定性=(1-服务连不通次数/天数)*100%

[0086] 稳定性=100%在基础积分的基础上增长15%

[0087] 稳定性>98%在基础积分的基础上增长10%

[0088] 稳定性>96%在基础积分的基础上增长5%

[0089] 稳定性>95%在基础积分的基础上增长0%

[0090] 稳定性>94%在基础积分的基础上增长-5%

[0091] 稳定性>92%在基础积分的基础上增长-10%

[0092] 稳定性>90%在基础积分的基础上增长-15%

[0093] 稳定性<90%在基础积分的基础上增长-20%

[0094] 根据好评率调整:

[0095] 好评率=(1-被投诉次数/总颁发数)*100%

[0096] 稳定性=100%在基础积分的基础上增长15%

[0097] 稳定性>95%在基础积分的基础上增长10%

[0098] 稳定性>90%在基础积分的基础上增长5%

[0099] 稳定性>85%在基础积分的基础上增长0%

[0100] 稳定性<80%在基础积分的基础上增长-5%

[0101] 稳定性<75%在基础积分的基础上增长-10%

[0102] 稳定性<70%在基础积分的基础上增长-15%

[0103] 注:如果成为信任锚后颁发的证书为零的话则不做调整。

[0104] 如图2所示,在上述实施例的基础上,本发明实施例中提供了一种可信声明系统中信任锚的管理装置,包括:获取模块21和选举模块22。其中,

[0105] 获取模块21用于获取区块链的各节点;

[0106] 选举模块22用于基于区块链的各节点,从候选信任锚池中选举出符合预设条件的候选信任锚作为信任锚;

[0107] 其中,所述预设条件包括所述候选信任锚在选举过程中得到的权益分排序在前第一预设数量内,或者所述候选信任锚在选举过程中得到的票数在前第二预设数量内,或者所述候选信任锚在选举过程中得到的信用分在前第三预设数量内。

[0108] 具体地,本发明实施例中提供的可信声明系统中信任锚的管理装置中各模块的作用与上述方法类实施例中各步骤的操作流程是一一对应的,实现的效果也是一致的,具体参见上述实施例,本发明实施例中对此不再赘述。

[0109] 在上述实施例的基础上,所述的可信声明系统中信任锚的管理装置,还包括:更新模块,所述更新模块用于:

[0110] 将所述信任锚添加至信任锚池;

[0111] 基于预设更新条件,对所述信任锚池进行更新;

[0112] 其中,所述预设更新条件包括预设更新周期和/或预设更新需求。

[0113] 图3所示,在上述实施例的基础上,本发明实施例中提供了一种电子设备,包括:处理器(processor)301、存储器(memory)302、通信接口(Communications Interface)303和通信总线304;其中,

[0114] 所述处理器301、存储器302、通信接口303通过通信总线304完成相互间的通信。所述存储器302存储有可被所述处理器301执行的程序指令,处理器301用于调用存储器302中的程序指令,以执行上述各方法实施例所提供的可信声明系统中信任锚的管理方法。

[0115] 需要说明的是,本实施例中的电子设备在具体实现时可以为服务器,也可以为PC机,还可以为其他设备,只要其结构中包括如图3所示的处理器301、通信接口303、存储器302和通信总线304,其中处理器301、通信接口303和存储器302通过通信总线304完成相互间的通信,且处理器301可以调用存储器302中的逻辑指令以执行上述方法即可。本实施例不对电子设备的具体实现形式进行限定。

[0116] 存储器302中的逻辑指令可以通过软件功能单元的形式实现并作为独立的产品销售或使用时,可以存储在一个计算机可读取存储介质中。基于这样的理解,本发明的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来,该计算机软件产品存储在一个存储介质中,包括若干指令用以使得一台计算机设备(可以是个人计算机,服务器,或者网络设备等)执行本发明各个实施例所述方法的全部或部分步骤。而前述的存储介质包括:U盘、移动硬盘、只读存储器(Read-Only Memory,ROM)、随机存取存储器(Random Access Memory,RAM)、磁碟或者光盘等各种可以存储程序代码的介质。

[0117] 进一步地,本发明实施例公开一种计算机程序产品,计算机程序产品包括存储在非暂态计算机可读存储介质上的计算机程序,计算机程序包括程序指令,当所述程序指令被计算机执行时,计算机能够执行上述各方法实施例所提供的可信声明系统中信任锚的管理方法。

[0118] 在上述实施例的基础上,本发明实施例还提供一种非暂态计算机可读存储介质,其上存储有计算机程序,该计算机程序被处理器执行时实现以执行上述各实施例提供的可信声明系统中信任锚的管理方法。

[0119] 以上所描述的装置实施例仅仅是示意性的,其中所述作为分离部件说明的单元可以是或者也可以不是物理上分开的,作为单元显示的部件可以是或者也可以不是物理单元,即可以位于一个地方,或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本实施例方案的目的。本领域普通技术人员在不付出创造性的劳动的情况下,即可以理解并实施。

[0120] 通过以上的实施方式的描述,本领域的技术人员可以清楚地了解到各实施方式可借助软件加必需的通用硬件平台的方式来实现,当然也可以通过硬件。基于这样的理解,上述技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来,该计算机软件产品可以存储在计算机可读存储介质中,如ROM/RAM、磁碟、光盘等,包括若干指令用以使得一台计算机设备(可以是个人计算机,服务器,或者网络设备等)执行各个实施例或者实施例的某些部分所述的方法。

[0121] 最后应说明的是:以上实施例仅用以说明本发明的技术方案,而非对其限制;尽管参照前述实施例对本发明进行了详细的说明,本领域的普通技术人员应当理解:其依然可

以对前述各实施例所记载的技术方案进行修改,或者对其中部分技术特征进行等同替换;而这些修改或者替换,并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围。

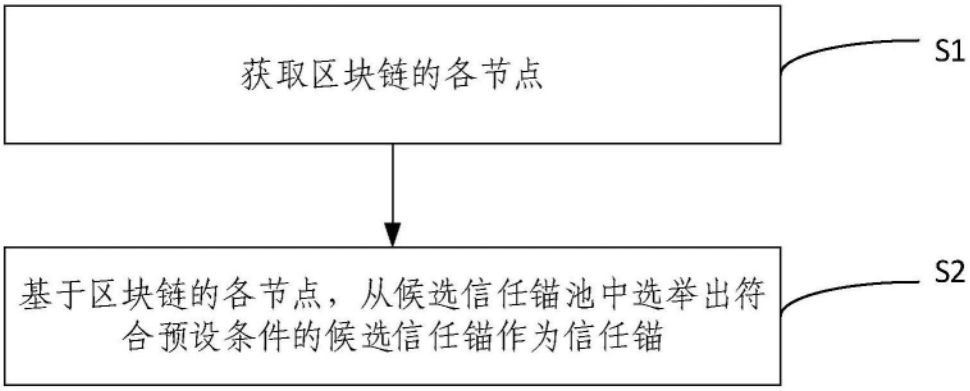

获取区块链的各节点
S1
基于区块链的各节点，从候选信任锚池中选举出符合预设条件的候选信任锚作为信任锚
S2

图1

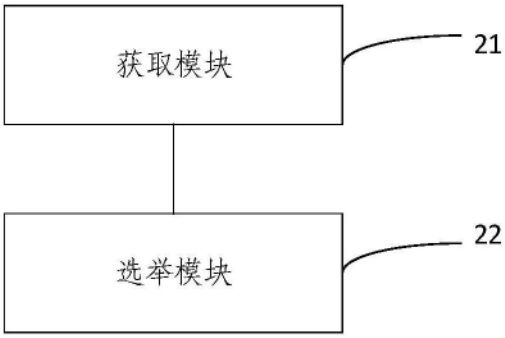

获取模块
21
选举模块
22

图2

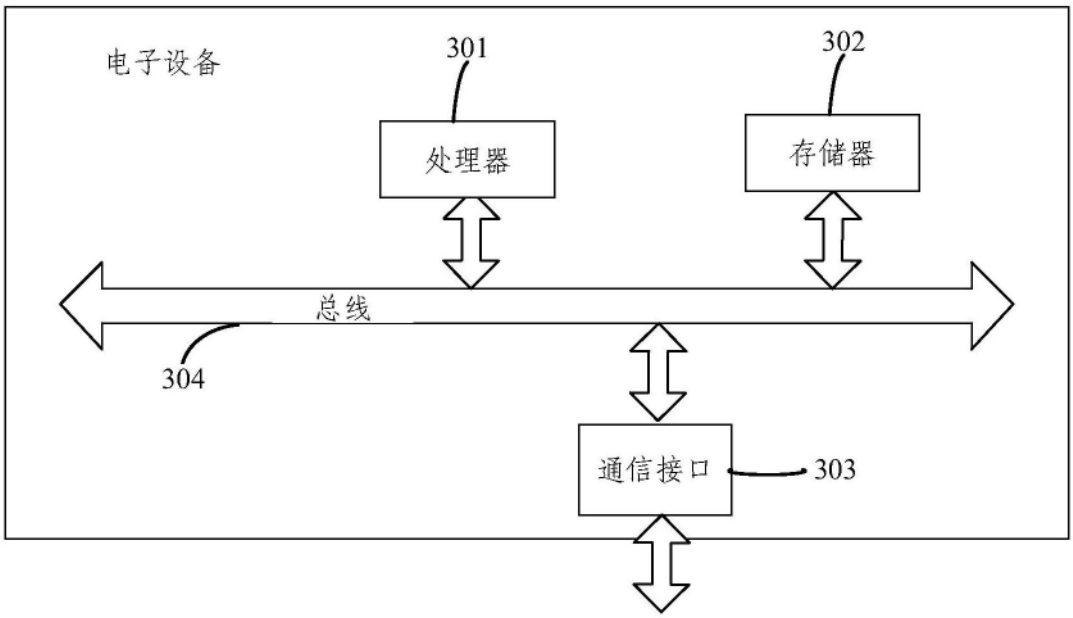

电子设备
301
处理器
302
存储器
总线
304
通信接口
303

图3