(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112132447 B
(45)授权公告日 2024.01.16

(21)申请号 202010992397.2

(22)申请日 2020.09.21

(65)同一申请的已公布的文献号
申请公布号 CN 112132447 A

(43)申请公布日 2020.12.25

(73)专利权人 江苏省未来网络创新研究院
地址 210000 江苏省南京市江宁开发区将军大道37号
专利权人 北京邮电大学

(72)发明人 谢人超 温瑶 贾庆民 黄韬

(74)专利代理机构 北京卓岚智财知识产权代理有限公司 11624
专利代理师 蒋真

(51)Int.Cl.
G06Q 10/0639(2023.01)
G06Q 20/38(2012.01)
G06Q 20/40(2012.01)

(56)对比文件
CN 109886791 A,2019.06.14
CN 110851531 A,2020.02.28
CN 111552573 A,2020.08.18
CN 108053239 A,2018.05.18
CN 110782343 A,2020.02.11
CN 111679905 A,2020.09.18
CN 111506932 A,2020.08.07
CN 111062807 A,2020.04.24
雷波.整合多方资源 算力网络有望实现计算资源利用率最优.通信世界.2020,(08),39-40.

审查员 陈龙

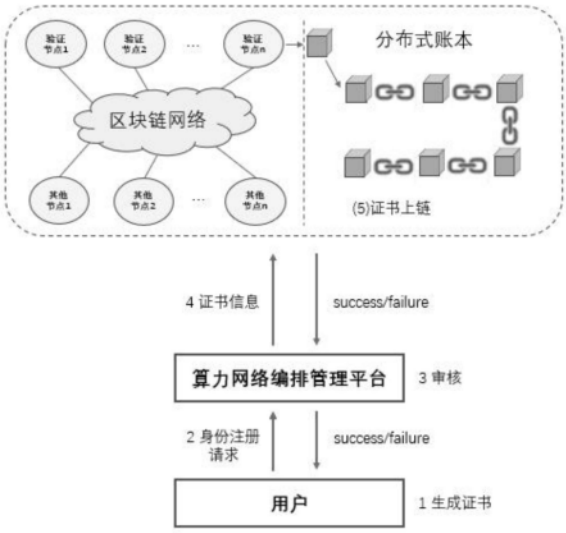
权利要求书3页 说明书8页 附图5页

(54)发明名称

一种基于区块链的算力网络信任评估与保障算法

(57)摘要

一种基于区块链的算力网络信任评估与保障算法,其特征是包括如下步骤:步骤(1)基于区块链的算力网络用户身份注册机制方法:算力网络中的用户包括算力提供方和算力消费方,算力消费方加入算力网络时,需完成身份注册;算力提供方加入算力网络时,需完成身份注册和算力服务注册;步骤(2)基于区块链的算力服务注册与感知机制方法:步骤(3)基于区块链的算力网络交易机制方法:步骤(4)基于区块链的信誉评估机制方法。本发明从用户和资源的身份信任、行为信任等多个维度建立详细的算力网络信任评估与保障体系,为算力网络的信任与安全管理提供支持。



CN 112132447 B

1.一种基于区块链的算力网络信任评估与保障方法,其特征是包括如下步骤:

步骤(1)基于区块链的算力网络用户身份注册机制方法:

算力网络中的用户包括算力提供方和算力消费方,算力消费方加入算力网络时,需完成身份注册;算力提供方加入算力网络时,需完成身份注册和算力服务注册;

步骤(2)基于区块链的算力服务注册与感知机制方法:

步骤(3)基于区块链的算力网络交易机制方法:

步骤(4)基于区块链的信誉评估机制方法:利用区块链技术的可追溯性,算力服务的信誉值通过历史交易评价分数计算得到,完成单次交易评估分数的计算,随后在此基础处上进行基于遗忘因子的时变信誉值计算方法;

所述步骤(1)的基于区块链的算力网络用户身份注册机制方法包括如下步骤:

步骤(1.1)用户生成一份数字证书,该证书需采用国际标准的X.509格式,且在扩展项中增加一个标识,便于查询;与证书相应的私钥存储于用户侧;

步骤(1.2)证书用户向算力网络编排管理平台发起身份注册请求,该请求包括用户的数字证书,以及验证证书所需的信息;如果证书实体用户申请的是个人实名证书,则还需提交用于证实其个人身份的信息;

步骤(1.3)算力网络编排管理平台收集用户的证书申请请求,并根据用户提交的信息验证证书的合法性,并结合算力网络准入规则,判定用户是否具有加入算力网络的资格;

步骤(1.4)若判定成功,将用户证书以“标识-证书-证书状态”的形式发送给区块链网络中的任一节点;若失败,则向用户返回注册失败信息;

步骤(1.5)用户证书信息发送至区块链网络后,由验证节点完成证书上链操作;验证节点将运行预设的区块链共识机制,将当前所有未纳入区块的“标识-证书-证书状态”作为区块链中的交易记录,打包成区块,并将区块发送给区块链所有节点;网络中其他节点接收到新区块后,验证区块以及区块中每条记录的正确性,如果正确,那么将该新区块加入到本地保存的分布式账本中;否则丢弃该新区块;

步骤(1.6)区块链网络完成证书上链操作后,向算力网络编排管理平台返回注册成功信息;随后,算力网络编排管理平台向用户通告身份注册成功信息;

所述步骤(2)基于区块链的算力服务注册与感知机制方法具体包括如下步骤:

步骤(2.1)算力提供方完成身份注册后,需继续向算力网络编排管理平台发送算力服务注册请求;注册请求中包含证书标识、证书、算力服务信息以及请求签名信息;算力信息包括静态特征信息和动态特征信息;静态信息一般在注册时就已固定,不轻易更改,主要包括服务IP及端口号、计算节点类型、CPU/GPU性能、存储容量、网络接口带宽、计费标准;动态特征主要包括一些计算负载信息,这些信息在算力交易过程中随时更新;

步骤(2.2)算力网络编排管理平台接收到算力服务注册请求后,根据证书标识向区块链节点查询在用户注册阶段存入分布式账本的用户证书及证书状态信息;

步骤(2.3)算力网络编排管理平台获得用户证书信息后,首先校验数字资质证书信息的合法性、有效性;证书的有效性验证包括证书是否处于有效期,证书名称是否与声称的名称一致;其次校验服务注册请求的签名信息,判断注册请求是否由该用户发出以及验证请求在传输过程中是否被篡改;若以上校验全数通过,算力网络编排管理平台将根据算力网络算力服务准入规则审核欲注册的算力服务;

步骤(2.4)若算力服务审核通过,则将进行以下操作:①根据算力服务注册信息为算力服务分配服务ID并给出服务的初始信誉值;初始信誉值根据用户的实名情况而定,信誉值随算力服务交易后的用户评价而改变;②将算力服务的信誉值以“标识-服务ID-初始信誉值”的形式发送给区块链节点,并由验证节点完成信誉值信息在区块链中的存储;③将算力服务信息存储至算力服务注册表中;④向用户返回算力服务注册成功信息;

步骤(2.5)若未通过步骤(2.3)中校验或者算力服务不具备准入资格,则向用户返回注册失败信息;

所述步骤(3)基于区块链的算力网络交易机制方法具体包括如下步骤:

步骤(3.1)算力消费方向算力网络编排管理平台发起服务请求,服务请求包括服务需求信息、用户的证书标识以及服务请求签名信息;

步骤(3.2)算力网络编排管理平台接收到该服务请求后,根据证书标识向区块链查询用户的证书信息;

步骤(3.3)获取用户的证书信息后,算力网络编排管理平台对数字资质证书信息的合法性和有效性和服务请求签名信息进行校验;该校验与算力服务注册中的校验相同;

步骤(3.4)用户身份信息验证通过后,算力网络编排管理平台将依据用户请求中的服务需求信息,选择算力服务调度策略,调度策略考虑用户对算力、网络、价格以及算力服务信誉值的综合需求,进行算力服务调度决策,为用户匹配最佳的算力提供方和网络连接;

步骤(3.5)算力网络编排管理平台完成调度决策后,将为交易双方制定服务电子合同;服务电子合同的内容包括算力消费方、算力提供方、资源需求信息、计费标准、服务售后条款信息;

步骤(3.6)算力网络编排管理平台生成服务电子合同后,将合同依次发送给用户以及服务提供方,双方以授权签名的形式签署合同,并将授权签名后的合同信息返回给编排管理平台;编排管理平台根据证书标识向区块链查询用户的证书信息,提取证书中的公钥对授权签名的合同信息进行校验;

步骤(3.7)校验通过后,将合同信息发送至区块链节点,并存储在区块链分布式账本中;

步骤(3.8)通过区块链智能合约维护服务电子合同,合同维护包括:交易结束后,①根据合同内的计费标准进行交易清算和资费转移;②收集用户对本次交易的提供方的评分和监管机构依据服务合同内容和提供方的完成程度对提供方的服务评分,基于以上两个评分值,得出提供方的本次交易评价分数,并根据基于遗忘因子的时变信誉值计算方法计算和更新提供方的信誉值。

2.根据权利要求1所述的一种基于区块链的算力网络信任评估与保障方法,其特征是所述步骤(2.5)之后还包括如下步骤:

服务启动之后,仍需定期向算力网络编排管理平台发送定期心跳,更新计算负载信息;若算力感知模块未收到来自服务的定期心跳,则会触发算力感知模块上注册表中实例的删除操作。

3.根据权利要求1所述的一种基于区块链的算力网络信任评估与保障方法,其特征是所述步骤(4)基于区块链的信誉评估机制方法具体包括如下步骤:

步骤(4.1)单次交易评价分数的方法:

单次交易评价由用户评价E_{trader}和监管机构评价E_{reg}两部分组成；

用户评价因素集合表示为$D=\{d_1,d_2,d_3,...,d_n\}$，n为评价因素的维度，评价因素包括计算完成度、耗时、价格合理度，每个评价因素的权重集表示为$W=\{w_1,w_2,w_3,...,w_n\}$，评价等级空间定义为$U=\{u_1,u_2,u_3,u_4,u_5,u_6\}$，其中$u_1,u_2,...,u_6$分别表示非常不满意、很不满意、不满意、满意、很满意、非常满意，所对应的量化值0,0.2,0.4,0.6,0.8,1；若用户对交易因素的评级为$R=\{r_1,r_2,r_3,...,r_n|r_n\in U\}$，则用户对一次交易的评价分数表示为：

$E_{trader}=W*R=(s_1,s_2,...,s_n)$；

另外，每当交易完成时，监管机构将提供方的完成情况与服务合同所约定的各项指标进行比对，并对服务给出评价分数E_{reg}；

以时间标识交易，在t时刻完成的交易所获得的评价分值表示为：

$E_{seller}(t)=wf_1\times Rep_{trader}(t)+wf_2\times Rep_{reg}(t)$

其中wf1、wf2是评价分量的权重因子；权重因子基于具体的交易类型进行调整；

步骤(4.2)基于遗忘因子的时变信誉值计算方法

基于Gambetta对信任的定义，采用基于遗忘因子的时变信誉值计算方法，以适应算力网络交易事件；在此计算方法中，最近的交易比之前的交易具有更高的计算权重；

由上述单次交易评价分数的介绍中可知，提供方在t_0-t_n时间内，所完成的每笔交易的评价分数表示为$E_{seller}(t_0)$，$E_{seller}(t_1)$，……，$E_{seller}(t_n)$，将这些评价分数加权累加即可得到提供方在t_n时刻的信誉值$R(t_n)$，表示为：

$$R(t_n)=\sum_{t=t_0}^{t=t_n}E_{seller}(t)\times\beta(t_n-t)$$

每笔交易评价分数的权重值$\beta(t_n-t)$因在时间上具有遗忘特性，即距离t_n时刻越近的交易评价分数具有更高的权重值，故称其为遗忘因子；$\beta(t)$是随时间增大而衰减的函数，$\beta(t)=e^{-f(t)}$。

一种基于区块链的算力网络信任评估与保障算法

技术领域

[0001] 本发明涉及信息技术领域,具体涉及一种基于区块链的算力网络信任评估与保障算法。

背景技术

[0002] 随着5G和人工智能的发展,未来社会中会在靠近用户的不同距离遍布许多不同规模的算力,通过全球网络为用户提供各类个性化的服务。从百亿量级的智能终端,到全球十亿量级的家庭网关,再到每个城市中未来MEC带来的数千个具备计算能力的边缘云,以及每个国家数十个大型的云DC,形成海量的泛在算力从各处接入互联网,构成云、边、端三级算力架构,并形成计算和网络深度融合的发展趋势。

[0003] 然而,在网络和计算融合的大趋势下,算力的部署与协同暴露出以下问题:

[0004] (1)边缘计算节点之间缺乏高效协同。边缘计算乃至泛在计算的场景中,单个站点的算力资源有限,而边缘站点之间又互不感知,无法协同工作,计算任务不能被调度至最优边缘节点进行计算。

[0005] (2)计算与网络缺乏高效协同。传统调度方案,例如目前的云网融合方案,业务应用层和网络解耦,应用层无法精准、实时地掌握网络的状态,以应用层为主的寻址结果的综合性能可能不是最优,甚至比较差,造成网络负载不均衡,业务不能被调度至最优边缘节点服务,导致业务体验差。

[0006] (3)云计算、边缘计算缺乏高效协同。起初,边缘计算旨在弥补现阶段部分应用场景下,中心云计算的一些短板;未来,“云边协同”将成为重要的发展趋势。如今5G边缘计算实际应用已陆续落地,但云边协同仍处于探索阶段。

[0007] 在此背景下,产业界提出了“算力网络”这一新型资源整合方案,通过网络分发服务节点的算力信息、存储信息、算法信息等,结合网络状态(如路径、时延)等信息,针对客户需求,提供最佳的资源分配及网络连接方案,并实现整网资源的最优化使用。

[0008] 然而,算力网络作为新兴概念,仍存在许多问题亟待解决。例如,如何保证计算资源的可信接入、如何评判服务请求的发起者是否可信;另外,用户需要频繁地使用算力网络中的计算资源和服务,因此如何在算力提供方和算力消费方之间进行可信的服务交易也成为一个未解决的重要课题。虽然各方积极推进算力网络的研究,但目前算力网络仍缺乏类似于云计算所具备的成熟的安全机制,这使得参与者的安全风险加大,并关系到算力网络是否真正走向应用。

[0009] 基于以上问题,本专利借助区块链技术的去中心化、可追溯、不可篡改、安全可靠等特性,拟开展基于区块链的算力网络关键技术研究,针对用户身份注册与认证、算力服务注册与认证、算力感知、算力调度与交易等过程中可能存在的安全可信问题,设计基于区块链的算力网络信任评估与保障机制。

[0010] 如图1,中国电信在前期理论研究的基础上组建了基于SDN、NFV、AI、云计算等新型技术的试验环境,并且结合AI赋能平台设计了可为AI应用提供灵活资源调度的“AI算力网

络”系统,其架构如图1所示。系统架构中主要包含4部分:算力网络管理编排系统、赋能平台、边缘/核心DC、网络基础设施。此外,AI算力网络采取类似于电网交易的交易流程,用户按照“提出需求-算力网络交易平台给出可选方案-用户选择方案-算力网络交易平台调度资源-交易结束后结算”的步骤,订购算力资源,获得相应的服务。AI算力网络能够自动分析用户提出的分级需求,并分配合适的基础资源。AI算力网络交易处理流程示例如图2所示。

[0011] 上述技术中,所提出的AI算力网络框架集中考虑了云、网、边三级算力深度融合和灵活调度的问题,而未考虑在算力网络中的安全可信问题。在大量异构资源接入和用户频繁使用算力网络计算资源的场景下,算力网络安全可信问题主要包括用户的可信身份认证、异构算力资源的可信接入、算力资源的可信服务以及高效可信的算力服务交易和结算等。

[0012] 如图3,基于边缘计算的核心挑战之一——隐私信任与安全保障问题,针对用户应用需求特征,优化了边缘计算系统。通过集成用户和资源的身份信任、行为信任、能力信任3个方面为综合信任度,构建了基于综合信任度的评估体系,设计并实现了基于综合信任的资源优化调度算法:移动资源感知(mobileresourceawareness,MRA)调度算法,该算法利用信任评估保障对边缘计算资源管理与协同优化。

[0013] 图3中的技术所提出的综合信任度适用于边缘计算场景,但并不完全适用于算力网络场景。现有技术二只是提出了身份信任的概念,并没有就如何实现身份信任给出具体的解决方案。其次,现有技术二提出行为信任与能力信任的评估方案过于简略,评估维度过于简单,且未验证该方案在重入攻击、共谋共计、不公平评级等情况下的性能。另外,该技术未就信任度的传输与存储展开研究,并未保证信任度的可追溯、不可篡改等特性。综上所述,该方案没有从根本上解决边缘计算的信任问题。

发明内容

[0014] 本发明提供的一种基于区块链的算力网络信任评估与保障算法从用户和资源的身份信任、行为信任等多个维度建立详细的算力网络信任评估与保障体系,为算力网络的信任与安全管理提供支持。

[0015] 本发明将围绕这些安全可信问题,展开研究。针对算力网络在用户身份注册与认证、算力服务注册与认证、算力感知、算力调度与交易中可能存在的安全可信问题,本发明拟借助区块链技术,分别设计基于区块链的算力网络用户身份注册机制、算力服务注册与感知机制、算力网络交易机制以及算力服务信誉评估机制,从而为算力网络安全可信提供解决方案。

[0016] 本发明的技术方案如下:

[0017] 一种基于区块链的算力网络信任评估与保障算法,包括如下步骤:

[0018] 步骤(1)基于区块链的算力网络用户身份注册机制方法:

[0019] 算力网络中的用户包括算力提供方和算力消费方,算力消费方加入算力网络时,需完成身份注册;算力提供方加入算力网络时,需完成身份注册和算力服务注册;

[0020] 步骤(2)基于区块链的算力服务注册与感知机制方法:

[0021] 步骤(3)基于区块链的算力网络交易机制方法:

[0022] 步骤(4)基于区块链的信誉评估机制方法:利用区块链技术的可追溯性,算力服务

的信誉值可通历史交易评价分数计算得到,完成单次交易评估分数的计算,随后在此基础处上进行基于遗忘因子的时变信誉值计算方法。

[0023] 所述步骤(1)的基于区块链的算力网络用户身份注册机制方法包括如下步骤:

[0024] 步骤(1.1)用户生成一份数字证书,该证书需采用国际标准的X.509格式,且在扩展项中增加一个标识,便于查询;与证书相应的私钥存储于用户侧;

[0025] 步骤(1.2)证书用户向算力网络编排管理平台发起身份注册请求,该请求包括用户的数字证书,以及验证证书所需的信息;如果证书实体用户申请的是个人实名证书,则还需提交用于证实其个人身份的信息,例如居民身份信息;

[0026] 步骤(1.3)算力网络编排管理平台收集用户的证书申请请求,并根据用户提交的信息验证证书的合法性,并结合算力网络准入规则,判定用户是否具有加入算力网络的资格;

[0027] 步骤(1.4)若判定成功,将用户证书以“标识-证书-证书状态”的形式发送给区块链网络中的任一节点;若失败,则向用户返回注册失败信息;

[0028] 步骤(1.5)用户证书信息发送至区块链网络后,由验证节点完成证书上链操作;验证节点将运行预设的区块链共识机制,将当前所有未纳入区块的“标识-证书-证书状态”作为区块链中的交易记录,打包成区块,并将区块发送给区块链所有节点;网络中其他节点接收到新区块后,验证区块以及区块中每条记录的正确性,如果正确,那么将该新区块加入到本地保存的分布式账本中;否则丢弃该新区块;

[0029] 步骤(1.6)区块链网络完成证书上链操作后,向算力网络编排管理平台返回注册成功信息;随后,算力网络编排管理平台向用户通告身份注册成功信息。

[0030] 所述步骤(2)基于区块链的算力服务注册与感知机制方法具体包括如下步骤:

[0031] 步骤(2.1)算力提供方完成身份注册后,需继续向算力网络编排管理平台发送算力服务注册请求。注册请求中包含证书标识、证书、算力服务信息以及请求签名信息。算力信息包括静态特征信息和动态特征信息。静态信息一般在注册时就已固定,不轻易更改,主要包括服务IP及端口号、计算节点类型、CPU/GPU性能、存储容量、网络接口带宽、计费标准等;动态特征主要包括一些计算负载信息,这些信息在算力交易过程中随时更新,例如当前在线的服务实例数量、CPU/GPU/内存使用率以及当前连接数等[5]。

[0032] 步骤(2.2)算力网络编排管理平台接收到算力服务注册请求后,根据证书标识向区块链节点查询在用户注册阶段存入分布式账本的用户证书及证书状态信息。

[0033] 步骤(2.3)算力网络编排管理平台获得用户证书信息后,首先校验数字资质证书信息的合法性、有效性。证书的有效性验证包括证书是否处于有效期,证书名称是否与声称的名称一致等;其次校验服务注册请求的签名信息,判断注册请求是否由该用户发出以及验证请求在传输过程中是否被篡改。若以上校验全数通过,算力网络编排管理平台将根据算力网络算力服务准入规则审核欲注册的算力服务。

[0034] 步骤(2.4)若算力服务审核通过,则将进行以下操作:①根据算力服务注册信息为算力服务分配服务ID并给出服务的初始信誉值。初始信誉值可根据用户的实名情况而定,信誉值随算力服务交易后的用户评价而改变,有关信誉值评定的内容详见第四小节所述的“基于区块链的信誉评估机制”;②将算力服务的信誉值以“标识-服务ID-初始信誉值”的形式发送给区块链节点,并由验证节点完成信誉值信息在区块链中的存储;③将算力服务信

息存储至算力服务注册表中;④向用户返回算力服务注册成功信息。

[0035] 步骤(2.5)若未通过步骤(2.3)中校验或者算力服务不具备准入资格,则向用户返回注册失败信息。

[0036] 所述步骤(2.5)之后还包括如下步骤:

[0037] 服务启动之后,仍需定期向算力网络编排管理平台发送定期心跳,更新计算负载信息;若算力感知模块未收到来自服务的定期心跳,则会触发算力感知模块上注册表中实例的删除操作。

[0038] 所述步骤(3)基于区块链的算力网络交易机制方法具体包括如下步骤:

[0039] 步骤(3.1)算力消费方向算力网络编排管理平台发起服务请求,服务请求包括服务需求信息、用户的证书标识以及服务请求签名信息;

[0040] 步骤(3.2)算力网络编排管理平台接收到该服务请求后,根据证书标识向区块链查询用户的证书信息;

[0041] 步骤(3.3)获取用户的证书信息后,算力网络编排管理平台对数字资质证书信息的合法性和有效性和服务请求签名信息进行校验。该校验与算力服务注册中的校验相同;

[0042] 步骤(3.4)用户身份信息验证通过后,算力网络编排管理平台将依据用户请求中的服务需求信息,选择算力服务调度策略(调度策略应考虑用户对算力、网络、价格以及算力服务信誉值的综合需求),进行算力服务调度决策,为用户匹配最佳的算力提供方和网络连接;

[0043] 步骤(3.5)算力网络编排管理平台完成调度决策后,将为交易双方制定服务电子合同;服务电子合同的内容包括算力消费方、算力提供方、资源需求信息、计费标准(例如按应用部署使用的时长或者调用次数进行计费)、服务售后条款信息等;

[0044] 步骤(3.6)算力网络编排管理平台生成服务电子合同后,将合同依次发送给用户以及服务提供方,双方以授权签名的形式签署合同,并将授权签名后的合同信息返回给编排管理平台;编排管理平台根据证书标识向区块链查询用户的证书信息,提取证书中的公钥对授权签名的合同信息进行校验;

[0045] 步骤(3.7)校验通过后,将合同信息发送至区块链节点,并存储在区块链分布式账本中;

[0046] 步骤(3.8)通过区块链智能合约维护服务电子合同,合同维护包括:交易结束后,①根据合同内的计费标准进行交易清算和资费转移;②收集用户对本次交易的提供方的评分和监管机构依据服务合同内容和提供方的完成程度对提供方的服务评分,基于以上两个评分值,得出提供方的本次交易评价分数,并根据基于遗忘因子的时变信誉值计算方法计算和更新提供方的信誉值。

[0047] 所述步骤(4)基于区块链的信誉评估机制方法具体包括如下步骤:

[0048] 步骤(4.1)单次交易评价分数的方法:

[0049] 单次交易评价由用户评价E_{trader}和监管机构评价E_{reg}两部分组成;

[0050] 用户评价因素集合可表示为$D=\{d_1,d_2,d_3,\ldots,d_n\}$(n为评价因素的维度,评价因素可为计算完成度、耗时、价格合理度等),每个评价因素的权重集可表示为$W=\{w_1,w_2,w_3,\ldots,w_n\}$,评价等级空间可定义为$U=\{u_1,u_2,u_3,u_4,u_5,u_6\}$,其中$u_1,u_2,\ldots,u_6$分别表示非常不满意、很不满意、不满意、满意、很满意、非常满意,所对应的量化值0,0.2,0.4,0.6,

0.8,1;若用户对交易因素的评级为$R=\{r_1,r_2,r_3,\ldots,r_n|r_n\in U\}$,则用户对一次交易的评价分数可表示为:

[0051] $E_{mader}=W*R=(s_1,s_2,\ldots,s_n)$;

[0052] 另外,每当交易完成时,监管机构将提供方的完成情况与服务合同所约定的各项指标进行比对,并对服务给出评价分数E_{reg};

[0053] 以时间标识交易,在t时刻完成的交易所获得的评价分值可表示为:

[0054] $E_{seller}(t)=wf_1\times Rep_{trader}(t)+wf_2\times Rep_{reg}(t)$

[0055] 其中wf1、wf2是评价分量的权重因子;权重因子可基于具体的交易类型进行调整;

[0056] 步骤(4.2)基于遗忘因子的时变信誉值计算方法

[0057] 基于Gambetta对信任的定义,本文采用基于遗忘因子的时变信誉值计算方法,以适应算力网络交易事件;在此计算方法中,最近的交易比之前的交易具有更高的计算权重;

[0058] 由上述单次交易评价分数的介绍中可知,提供方在t_0-t_n时间内,所完成的每笔交易的评价分数可表示为$E_{seller}(t_0)$,$E_{seller}(t_1)$,……,$E_{seller}(t_n)$,将这些评价分数加权累加即可得到提供方在t_n时刻的信誉值$R(t_n)$,可表示为:

[0059] $$R(t_n)=\sum_{t=t_0}^{t=t_n}E_{seller}(t)\times\beta(t_n-t)$$

[0060] 每笔交易评价分数的权重值$\beta(t_n-t)$因在时间上具有遗忘特性,即距离t_n时刻越近的交易评价分数具有更高的权重值,故称其为遗忘因子;$\beta(t)$应是随时间增大而衰减的函数,例如$\beta(t)=e^{-f(t)}$。

[0061] 本发明的有益效果如下:

[0062] 本发明借助区块链的去中心化、可追溯、不可篡改、安全可靠等特性,研究了集中式算力网络架构下的算力网络用户身份注册与认证,算力服务注册、认证与感知,算力网络交易机制,算力网络信誉评估机制等算力网络关键技术,有效防范了重入攻击、共谋攻击与不公平评级等作恶行为,保障了用户、算力资源的可信接入和算力提供方与算力消费方的可信交易,为算力网络的信任评估与保障提供支持。

[0063] 基于区块链的算力网络用户身份注册与认证机制。本发明提出了算力网络中,算力资源提供方和算力网络资源消费方的身份注册与认证机制,有效防范算力网络交易中的可能遭受的重入攻击。

[0064] 基于区块链的算力服务注册与感知机制。本发明提出了算力网络中,算力服务的注册与感知机制,确保异构资源的可信接入,为算力网络提供可信接入保障。

[0065] 基于区块链的算力网络交易机制。

[0066] 本发明提出了算力网络中的可信交易机制,基于算力网络编排管理平台的调度,结合区块链智能合约,保证算力网络的可信交易与可信结算。

[0067] 基于区块链的信誉评估机制。本发明提出了基于遗忘因子的算力网络信誉值评估机制,有效防范算力网络交易过程可能遭受的共谋攻击与不公平评级,保障算力网络可信交易。

附图说明

[0068] 图1为现有技术的AI算力网络框架示意图。

[0069] 图2为现有技术的AI网络业务处理流程示意图。

[0070] 图3为现有技术的边缘计算信任保障体系示意图。

[0071] 图4本发明的算力网络用户注册流程示意图。

[0072] 图5本发明的算力网络算力服务注册流程示意图。

[0073] 图6为本发明的算力网络交易流程示意图。

具体实施方式

[0074] 下面结合附图对本发明做进一步说明。

[0075] 如图4至图6,一种基于区块链的算力网络信任评估与保障算法,包括如下步骤:

[0076] 步骤(1)基于区块链的算力网络用户身份注册机制方法:

[0077] 算力网络中的用户包括算力提供方和算力消费方,算力消费方加入算力网络时,需完成身份注册;算力提供方加入算力网络时,需完成身份注册和算力服务注册;

[0078] 步骤(2)基于区块链的算力服务注册与感知机制方法:

[0079] 步骤(3)基于区块链的算力网络交易机制方法:

[0080] 步骤(4)基于区块链的信誉评估机制方法:利用区块链技术的可追溯性,算力服务的信誉值可通历史交易评价分数计算得到,完成单次交易评估分数的计算,随后在此基础处上进行基于遗忘因子的时变信誉值计算方法。

[0081] 所述步骤(1)的基于区块链的算力网络用户身份注册机制方法包括如下步骤:

[0082] 步骤(1.1)用户生成一份数字证书,该证书需采用国际标准的X.509格式,且在扩展项中增加一个标识,便于查询;与证书相应的私钥存储于用户侧;

[0083] 步骤(1.2)证书用户向算力网络编排管理平台发起身份注册请求,该请求包括用户的数字证书,以及验证证书所需的信息;如果证书实体用户申请的是个人实名证书,则还需提交用于证实其个人身份的信息,例如居民身份信息;

[0084] 步骤(1.3)算力网络编排管理平台收集用户的证书申请请求,并根据用户提交的信息验证证书的合法性,并结合算力网络准入规则,判定用户是否具有加入算力网络的资格;

[0085] 步骤(1.4)若判定成功,将用户证书以“标识-证书-证书状态”的形式发送给区块链网络中的任一节点;若失败,则向用户返回注册失败信息;

[0086] 步骤(1.5)用户证书信息发送至区块链网络后,由验证节点完成证书上链操作;验证节点将运行预设的区块链共识机制,将当前所有未纳入区块的“标识-证书-证书状态”作为区块链中的交易记录,打包成区块,并将区块发送给区块链所有节点;网络中其他节点接收到新区块后,验证区块以及区块中每条记录的正确性,如果正确,那么将该新区块加入到本地保存的分布式账本中;否则丢弃该新区块;

[0087] 步骤(1.6)区块链网络完成证书上链操作后,向算力网络编排管理平台返回注册成功信息;随后,算力网络编排管理平台向用户通告身份注册成功信息。

[0088] 所述步骤(2)基于区块链的算力服务注册与感知机制方法具体包括如下步骤:

[0089] 步骤(2.1)算力提供方完成身份注册后,需继续向算力网络编排管理平台发送算力服务注册请求。注册请求中包含证书标识、证书、算力服务信息以及请求签名信息。算力信息包括静态特征信息和动态特征信息。静态信息一般在注册时就已固定,不轻易更改,主

要包括服务IP及端口号、计算节点类型、CPU/GPU性能、存储容量、网络接口带宽、计费标准等;动态特征主要包括一些计算负载信息,这些信息在算力交易过程中随时更新,例如当前在线的服务实例数量、CPU/GPU/内存使用率以及当前连接数等[5]。

[0090] 步骤(2.2)算力网络编排管理平台接收到算力服务注册请求后,根据证书标识向区块链节点查询在用户注册阶段存入分布式账本的用户证书及证书状态信息。

[0091] 步骤(2.3)算力网络编排管理平台获得用户证书信息后,首先校验数字资质证书信息的合法性、有效性。证书的有效性验证包括证书是否处于有效期,证书名称是否与声称的名称一致等;其次校验服务注册请求的签名信息,判断注册请求是否由该用户发出以及验证请求在传输过程中是否被篡改。若以上校验全数通过,算力网络编排管理平台将根据算力网络算力服务准入规则审核欲注册的算力服务。

[0092] 步骤(2.4)若算力服务审核通过,则将进行以下操作:①根据算力服务注册信息为算力服务分配服务ID并给出服务的初始信誉值。初始信誉值可根据用户的实名情况而定,信誉值随算力服务交易后的用户评价而改变,有关信誉值评定的内容详见第四小节所述的“基于区块链的信誉评估机制”;②将算力服务的信誉值以“标识-服务ID-初始信誉值”的形式发送给区块链节点,并由验证节点完成信誉值信息在区块链中的存储;③将算力服务信息存储至算力服务注册表中;④向用户返回算力服务注册成功信息。

[0093] 步骤(2.5)若未通过步骤(2.3)中校验或者算力服务不具备准入资格,则向用户返回注册失败信息。

[0094] 所述步骤(2.5)之后还包括如下步骤:

[0095] 服务启动之后,仍需定期向算力网络编排管理平台发送定期心跳,更新计算负载信息;若算力感知模块未收到来自服务的定期心跳,则会触发算力感知模块上注册表中实例的删除操作。

[0096] 所述步骤(3)基于区块链的算力网络交易机制方法具体包括如下步骤:

[0097] 步骤(3.1)算力消费方向算力网络编排管理平台发起服务请求,服务请求包括服务需求信息、用户的证书标识以及服务请求签名信息;

[0098] 步骤(3.2)算力网络编排管理平台接收到该服务请求后,根据证书标识向区块链查询用户的证书信息;

[0099] 步骤(3.3)获取用户的证书信息后,算力网络编排管理平台对数字资质证书信息的合法性和有效性和服务请求签名信息进行校验。该校验与算力服务注册中的校验相同;

[0100] 步骤(3.4)用户身份信息验证通过后,算力网络编排管理平台将依据用户请求中的服务需求信息,选择算力服务调度策略(调度策略应考虑用户对算力、网络、价格以及算力服务信誉值的综合需求),进行算力服务调度决策,为用户匹配最佳的算力提供方和网络连接;

[0101] 步骤(3.5)算力网络编排管理平台完成调度决策后,将为交易双方制定服务电子合同;服务电子合同的内容包括算力消费方、算力提供方、资源需求信息、计费标准(例如按应用部署使用的时长或者调用次数进行计费)、服务售后条款信息等;

[0102] 步骤(3.6)算力网络编排管理平台生成服务电子合同后,将合同依次发送给用户以及服务提供方,双方以授权签名的形式签署合同,并将授权签名后的合同信息返回给编排管理平台;编排管理平台根据证书标识向区块链查询用户的证书信息,提取证书中的公

钥对授权签名的合同信息进行校验；

[0103] 步骤(3.7)校验通过后，将合同信息发送至区块链节点，并存储在区块链分布式账本中；

[0104] 步骤(3.8)通过区块链智能合约维护服务电子合同，合同维护包括：交易结束后，①根据合同内的计费标准进行交易清算和资费转移；②收集用户对本次交易的提供方的评分和监管机构依据服务合同内容和提供方的完成程度对提供方的服务评分，基于以上两个评分值，得出提供方的本次交易评价分数，并根据基于遗忘因子的时变信誉值计算方法计算和更新提供方的信誉值。

[0105] 所述步骤(4)基于区块链的信誉评估机制方法具体包括如下步骤：

[0106] 步骤(4.1)单次交易评价分数的方法：

[0107] 单次交易评价由用户评价E_{trader}和监管机构评价E_{reg}两部分组成；

[0108] 用户评价因素集合可表示为$D=\{d_1,d_2,d_3,\ldots,d_n\}$(n为评价因素的维度，评价因素可为计算完成度、耗时、价格合理度等)，每个评价因素的权重集可表示为$W=\{w_1,w_2,w_3,\ldots,w_n\}$，评价等级空间可定义为$U=\{u_1,u_2,u_3,u_4,u_5,u_6\}$，其中$u_1,u_2,\ldots,u_6$分别表示非常不满意、很不满意、不满意、满意、很满意、非常满意，所对应的量化值0,0.2,0.4,0.6,0.8,1；若用户对交易因素的评级为$R=\{r_1,r_2,r_3,\ldots,r_n|r_n\in U\}$，则用户对一次交易的评价分数可表示为：

[0109] $E_{mader}=W*R=(s_1,s_2,\cdots,s_n)$；

[0110] 另外，每当交易完成时，监管机构将提供方的完成情况与服务合同所约定的各项指标进行比对，并对服务给出评价分数E_{reg}；

[0111] 以时间标识交易，在t时刻完成的交易所获得的评价分值可表示为：

[0112] $E_{seller}(t)=wf_1\times Rep_{trader}(t)+wf_2\times Rep_{reg}(t)$

[0113] 其中wf1、wf2是评价分量的权重因子；权重因子可基于具体的交易类型进行调整；

[0114] 步骤(4.2)基于遗忘因子的时变信誉值计算方法

[0115] 基于Gambetta对信任的定义，本文采用基于遗忘因子的时变信誉值计算方法，以适应算力网络交易事件；在此计算方法中，最近的交易比之前的交易具有更高的计算权重；

[0116] 由上述单次交易评价分数的介绍中可知，提供方在t_0-t_n时间内，所完成的每笔交易的评价分数可表示为$E_{seller}(t_0)$，$E_{seller}(t_1)$，……，$E_{seller}(t_n)$，将这些评价分数加权累加即可得到提供方在t_n时刻的信誉值$R(t_n)$，可表示为：

[0117] $$R(t_n)=\sum_{t=t_0}^{t=t_n}E_{seller}(t)\times\beta(t_n-t)$$

[0118] 每笔交易评价分数的权重值$\beta(t_n-t)$因在时间上具有遗忘特性，即距离t_n时刻越近的交易评价分数具有更高的权重值，故称其为遗忘因子；$\beta(t)$应是随时间增大而衰减的函数，例如$\beta(t)=e^{-f(t)}$。

[0119] 以上显示和描述了本发明的基本原理、主要特征和本发明的优点。本行业的技术人员应该了解，本发明不受上述实施例的限制，上述实施例和说明书中描述的仅为本发明的优选例，并不用来限制本发明，在不脱离本发明精神和范围的前提下，本发明还会有各种变化和改进，这些变化和改进都落入要求保护的本发明范围内。本发明要求保护范围由所附的权利要求书及其等效物界定。

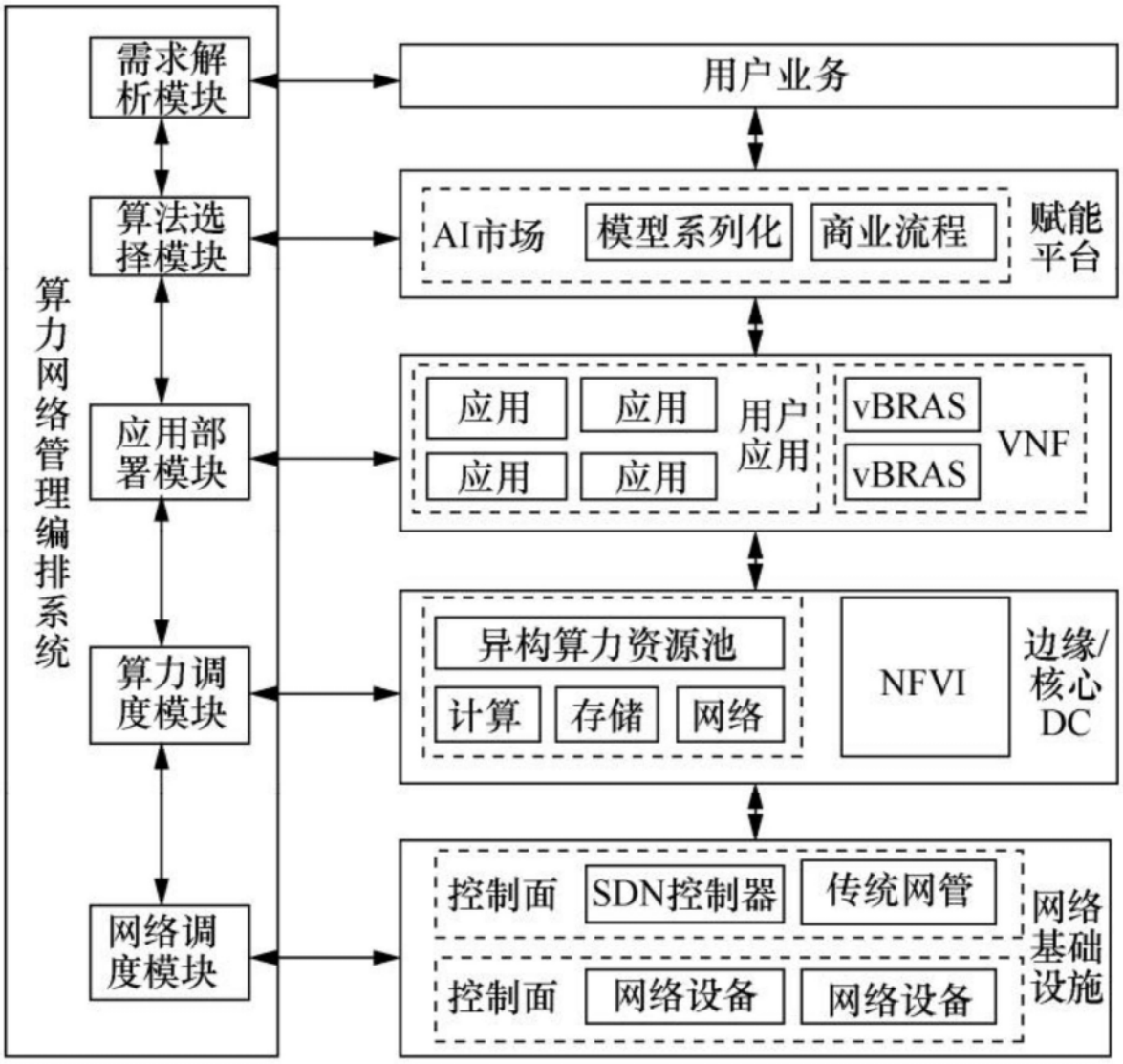

算力网络管理编排系统
需求解析模块
算法选择模块
应用部署模块
算力调度模块
网络调度模块
用户业务
AI市场
模型系列化
商业流程
赋能平台
应用
应用
应用
应用
用户应用
vBRAS
vBRAS
VNF
异构算力资源池
计算
存储
网络
NFVI
边缘/核心DC
控制面
SDN控制器
传统网管
控制面
网络设备
网络设备
网络基础设施

图1

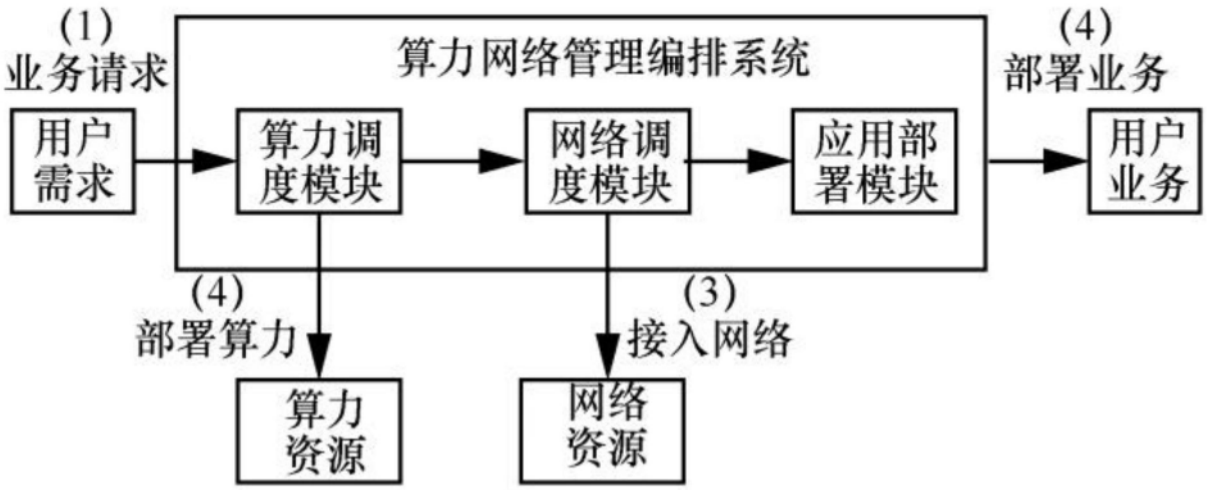

(1)
业务请求
算力网络管理编排系统
(4)
部署业务
用户需求
算力调度模块
网络调度模块
应用部署模块
用户业务
(4)
部署算力
(3)
接入网络
算力资源
网络资源

图2

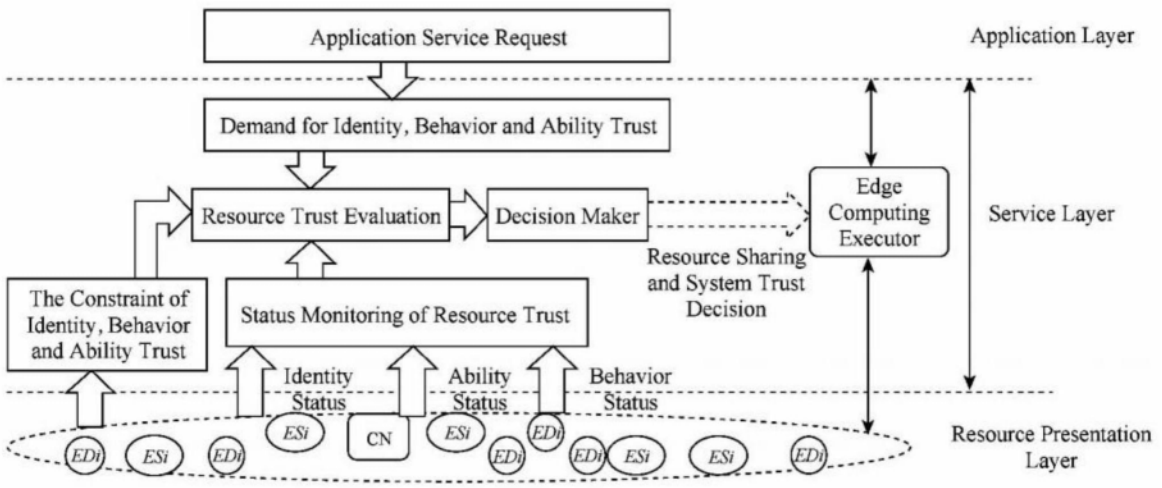

Application Service Request
Application Layer
Demand for Identity, Behavior and Ability Trust
Resource Trust Evaluation
Decision Maker
Edge Computing Executor
Service Layer
Resource Sharing and System Trust Decision
The Constraint of Identity, Behavior and Ability Trust
Status Monitoring of Resource Trust
Identity Status
Ability Status
Behavior Status
ESi
CN
EDi
Resource Presentation Layer

图3

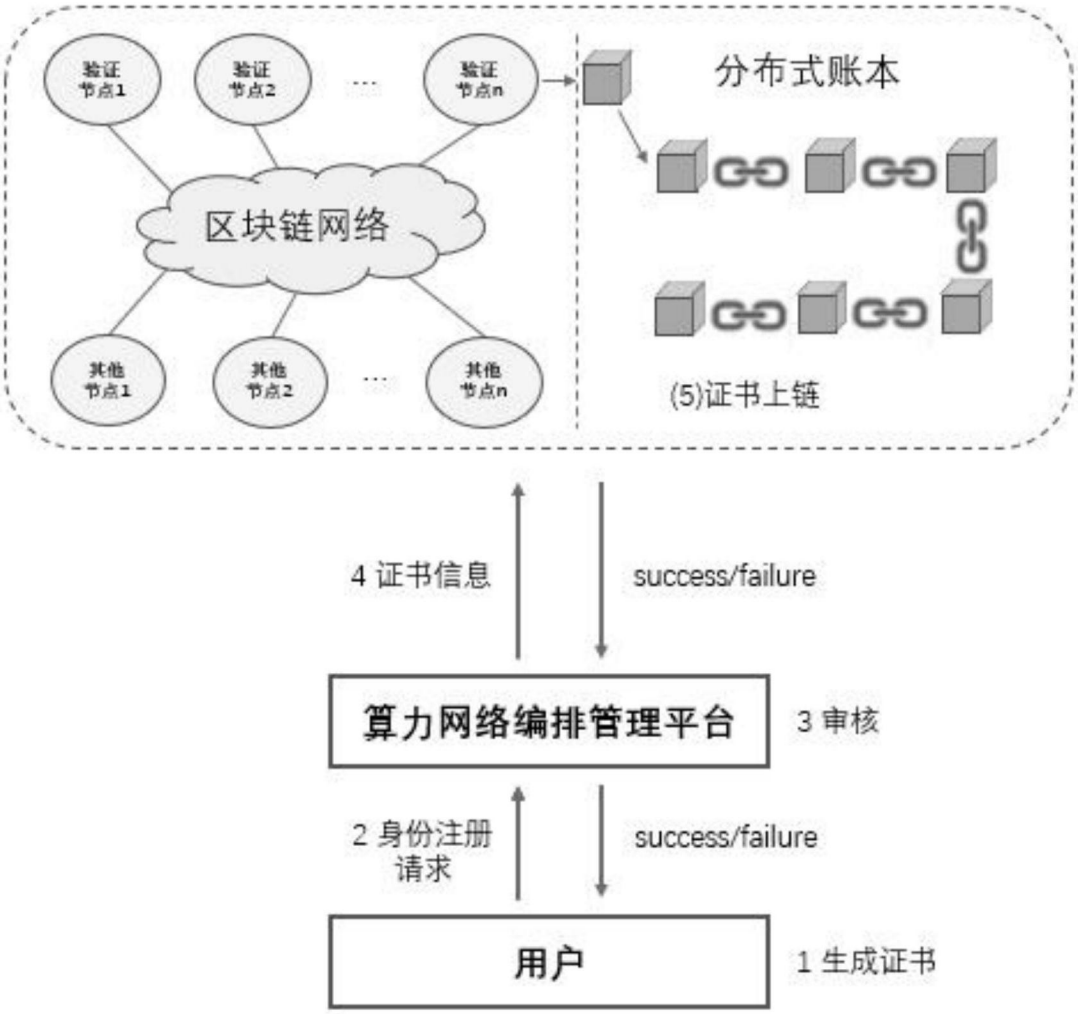

验证节点1
验证节点2
…
验证节点n
区块链网络
其他节点1
其他节点2
…
其他节点n
分布式账本
(5)证书上链
4 证书信息
success/failure
算力网络编排管理平台
3 审核
2 身份注册请求
success/failure
用户
1 生成证书

图4

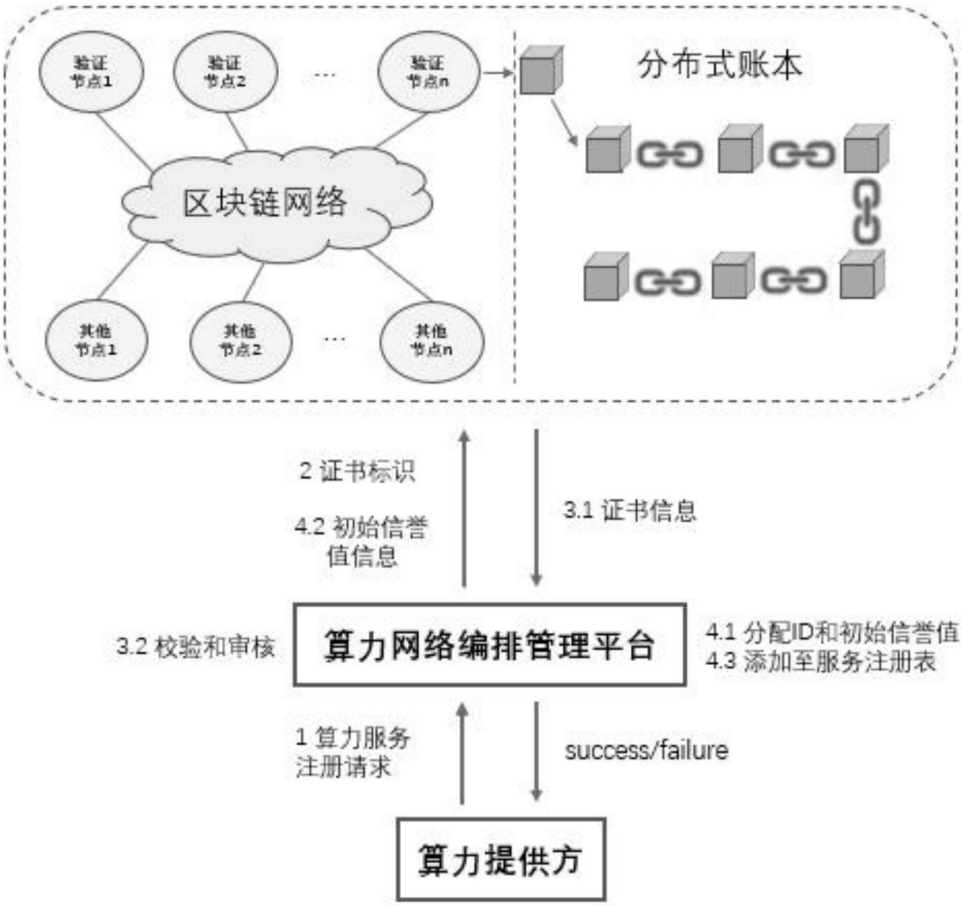

验证节点1
验证节点2
…
验证节点n
区块链网络
其他节点1
其他节点2
…
其他节点n
分布式账本
2 证书标识
4.2 初始信誉值信息
3.1 证书信息
3.2 校验和审核
算力网络编排管理平台
4.1 分配ID和初始信誉值
4.3 添加至服务注册表
1 算力服务注册请求
success/failure
算力提供方

图5

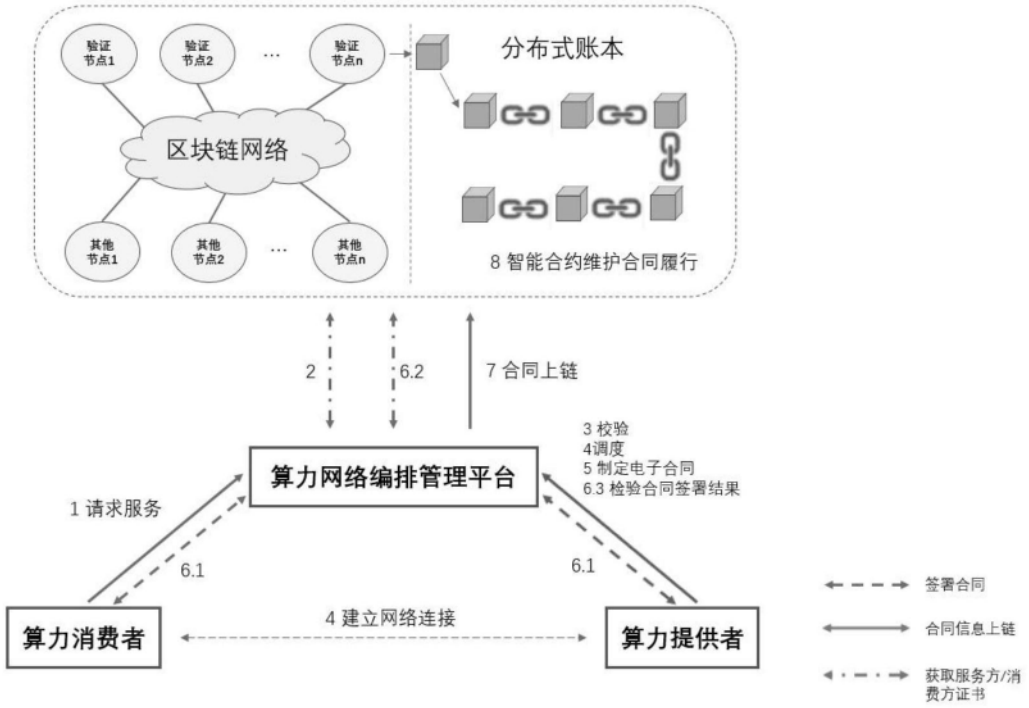

验证节点1
验证节点2
验证节点n
区块链网络
其他节点1
其他节点2
其他节点n
分布式账本
8 智能合约维护合同履行
2
6.2
7 合同上链
3 校验
4调度
5 制定电子合同
6.3 检验合同签署结果
算力网络编排管理平台
1 请求服务
6.1
6.1
4 建立网络连接
算力消费者
算力提供者
签署合同
合同信息上链
获取服务方/消费方证书

图6