doi:10.14132/j.cnki.1673-5439.2021.04.013

融合区块链的算力网络信任评估与保障方案研究

温 瑶[1], 陆晶晶[2], 卢 华[2], 谢人超[1]

(1.北京邮电大学 网络与交换国家重点实验室,北京 100876
2.广东省新一代通信与网络创新研究院 网络技术创新中心,广东 广州 510000)

摘要:算力网络是通过网络承载、传递泛在计算服务,实现计算、网络融合一体化的新型网络架构。为实现安全可信的算力共享,借助区块链技术,提出了融合区块链的算力网络架构,并基于该架构设计了包含用户身份认证机制、算力服务注册机制、交易机制、信誉评估机制的信任评估与保障方案。仿真结果表明,该方案可为算力网络的算力资源共享提供安全可信保障。

关键词:算力网络;区块链;安全;信任

中图分类号:TP393 **文献标志码**:A **文章编号**:1673-5439(2021)04-0099-08

Blockchain-based trust evaluation and guarantee scheme for computing power network

WEN Yao[1], LU Jingjing[2], LU Hua[2], XIE Renchao[1]

(1.State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China
2.Center of Network Technology Innovation, Guangdong Communication & Network Institute, Guangzhou 510000, China)

Abstract: The computing power network is a new network architecture for realizing computing and network integration by carrying and delivering ubiquitous computing services in the network. To realize safe and reliable computing power sharing, a computing power network architecture integrating blockchain is proposed with the blockchain technology. Under this architecture, a trust evaluation and guarantee scheme, including mechanism of the user identity registration, the computing power registration and perception, and the transaction and reputation evaluation, is designed. Simulation results show that the scheme can provide a safe and credible guarantee for the computing power resource sharing in the computing power network.

Keywords: computing power network; blockchain; security; trust

随着5G时代的到来,5G网络的大带宽、低时延、海量连接将赋能千行百业。作为5G网络的核心基础设施,多接入边缘计算(Multi-access Edge Computing,MEC)将为未来工业互联网、大数据、人工智能等新型业务提供灵活的就近接入、低时延、高可靠等极致体验[1]。据预测,到2022年,全球边缘计算规模将与云计算不相上下[2]。与此同时,世界上对于6G技术的研究也已起步,虽然6G世界的蓝图尚未明确,但可以预见,6G时代人们所期盼的业务将以强大的信息处理能力,即算力为基础[2-3]。未来社会将会在靠近用户的不同位置部署许多不同规模的算力资源,通过全球网络为用户提供各类个性化的服务。大型云数据中心、具备云计算能力的MEC节点、全球十亿量级的家庭网关以及百亿量级的智能终端将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,从而形成计算和网

收稿日期:2021-02-28;修回日期:2021-04-10 本刊网址:http://nyzr.njupt.edu.cn
基金项目:国家重点研发计划(2019YFB1804403)资助项目
作者简介:温瑶,女,硕士研究生;陆晶晶(通信作者),女,工程师,lujingjing@gdcni.cn
引用本文:温瑶,陆晶晶,卢华,等.融合区块链的算力网络信任评估与保障方案研究[J].南京邮电大学学报(自然科学版),2021,41(4):99-106.

络深度融合的发展趋势[4]。在此趋势下,算力的部署与协同暴露出以下问题:计算与网络之间,云计算与边缘计算节点之间以及边缘计算节点之间均缺乏高效协同。在此背景下,业界提出了“算力网络”[4-6]这一新型网络架构。

然而,算力网络中资源设备的高度异构和广泛分布预计会对算力共享过程中的用户身份认证和算力资源接入造成巨大的安全威胁。另外,算力资源共享或交易时,需评估和保证计算任务可以被身份可信、行为可信、服务质量满足需求的能力可信的算力资源设备完成,但目前算力网络仍缺乏算力资源设备的信任管理方案。其次,如何实现算力的可信交易以及交易记录的安全、可追溯存储也仍是一个未解决的重要课题。

区块链是一种分布式账本技术,能够在不完全可信的环境下,实现陌生节点之间点对点的价值传递[7-8]。针对前文提到的算力网络中存在的安全和信任问题,本文借助区块链的去中心化、可追溯、不可篡改、安全可靠等特性,提出了基于区块链的算力网络逻辑架构和网络架构,并研究了该架构下的用户身份注册机制、算力服务注册机制、交易机制、信誉评估机制等关键技术,从用户、资源的身份信任、能力信任等多个维度建立了算力网络信任评估与保障方案。

本文的主要贡献包括 3 个方面:

(1) 为使区块链赋能算力网络,本文首先提出了融合区块链的算力网络架构,架构包括逻辑架构与网络架构。

(2) 在所提架构的基础之上,本文提出了基于区块链的信任评估与保障方案。首先,为保证服务请求发起者的可信性,该方案提出了基于区块链的算力网络用户身份注册机制;其次,为保障算力资源的可信接入,该方案设计了算力服务注册机制;再次,为达成算力网络交易记录不可篡改、可追溯,利用区块链智能合约技术,该方案提出了基于区块链的算力网络交易机制;最后,为公平评估算力资源设备的服务质量,监控资源提供方的服务可靠性,该方案设计了算力网络算力服务信誉值评估机制。

(3) 对所提架构及方案进行了仿真和安全性能分析。

1 相关工作

目前算力网络的研究重心还在架构设计以及控制技术上,少有文献针对算力网络的安全和信任管理展开研究。中国联通[5]提出了一种设想的 MEC+区块链的算力网络资源交易过程,以满足监管、审计的需要。雷波等[6]类比电力交易的商业模式,描述了算力网络中用户订购算力、获取相应服务的流程,并提出了借助区块链等新兴技术实现算力网络交易平台的设想。

然而,安全和信任管理已广泛地应用于物联网、P2P 网络、边缘计算等多种场景。Lahbib 等[9]提出了在物联网中考虑节点和链路信任计算物联网实体的准确信任值,但该方案将信任相关信息存储在一个中心化实体中,容易引发隐私泄露等安全问题。Wang 等[10]提出了基于贝叶斯网络的信任模型和基于推荐算法的信誉评估方法,但未考虑信任信息的收集、存储过程中的完整性和不可篡改性。邓晓衡等[11]针对边缘计算场景下的隐私信任与安全保障问题,定义了用户和资源的综合信任度,构建了资源和用户的多维信任评价机制,但该机制未将标识链接到单个实体,无法防止恶意实体伪造不同身份的欺骗行为。

同时,区块链凭借其独有的信任建立机制迅速覆盖了资源共享、数据存储、信誉系统等众多安全服务领域,并有望从根本上解决安全和信任管理问题[12]。Pan 等[13]提出了一种基于区块链和智能合约的“边缘计算-物联网”框架:EdgeChain,将边缘计算资源与物联网设备的身份、资源使用情况以及行为链接在一起,将边缘计算资源的活动和交易都记录在区块链的分布式账本中,实现信任相关信息的安全可信存储。Kang 等[14]利用区块链建立分布式数据库来管理车辆数据,并设计了基于信誉的数据源筛选方法,供车辆选择高质量、高可信的数据提供方,确保数据存储和数据共享的安全性。Khaqqi 等[15]提出了一个将区块链技术与可信交易相结合的排放交易机制(ETS)模型,以解决排放交易机制中的欺诈和管理问题,但该模型中的卖家信誉值仅由审计机构评定,存在不公平性。Chen 等[16]提出了在资源受限条件下只存储设备信誉最大值的信誉系统;Malik 等[17]针对供应链场景提出了“信任链”,跟踪供应链参与者之间的每一次交互,并基于全部交互行为动态评估信任。Moinet 等[18]提出了一种自治无线传感器网络环境下的信任模型,该模型中的节点必须保持一定信誉值才能继续参与网络,但此模型仅在网络节点级别上进行信任评估,而在节点提供多个服务的情况下,无法对单个服务进行可信性评估,缺乏粒度。

综上所述,虽然业界提出了在交易模式上可以

考虑算力网络与区块链技术相结合,但未对其架构及交易机制进行详细设计,并且未考虑到算力网络中所存在的身份认证、数据安全存储与共享、信任管理等安全可信问题。而现有基于区块链的安全、信任管理方案大多基于特定场景和模式设计,并不完全适用算力网络架构和运行模式。因此,本文在当前研究工作的基础之上,首先提出了融合区块链的算力网络架构;并以此架构为基础,针对算力网络信任评估与保障方案展开设计。

2　融合区块链的算力网络架构

针对算力网络中存在的安全可信问题,本文借助区块链技术设计算力网络信任评估与保障方案。作为方案的基础,本节将首先提出融合区块链的算力网络架构。

如图 1 所示,融合区块链的算力网络架构分为算力网络编排管理平台、区块链可信运营平台、算力基础设施、网络基础设施及用户业务接入平台。

(1) 算力网络编排管理平台

算力网络编排管理平台采用 SDN/NFV 技术实现算力编排、网络编排及用户身份管理,该平台集中收集全网的算力资源、网络资源的状态信息并感知其变化,形成网络、算力拓扑;收集用户需求信息,抽象计算后,根据算力、网络的资源分配策略,实现算力与网络的同步化、最优化匹配和调度。另外,该平台还包括用户的身份注册和身份认证等身份管理功能。

(2) 区块链可信运营平台

可信运营平台主要由区块链技术实现。主要功能包括:采用区块链分布式账本及共识机制,安全可靠地存储用户信息、算力信息、交易电子合同等信息;采用区块链智能合约技术,维护交易电子合同的执行并在交易结束后,完成交易清算并更新算力服务信誉值。

(3) 算力基础设施

算力基础设施包含运营商自建、合营的核心数据中心与 MEC 节点,泛在端算力等算力资源。另外,异构资源统一管理模块屏蔽算力资源的异构属性。

(4) 网络基础设施

网络基础设施主要为连接用户和云、边、端算力的网络基础设施,包括控制面的 SDN 控制器、传统网管以及转发面的网络设备。

(5) 用户业务接入平台

用户业务接入平台为用户发布服务需求的入口。该层可屏蔽底层异构计算资源或不同网络连接类型的差异性,并根据用户所提出的算力、网络需求,为用户业务分级。

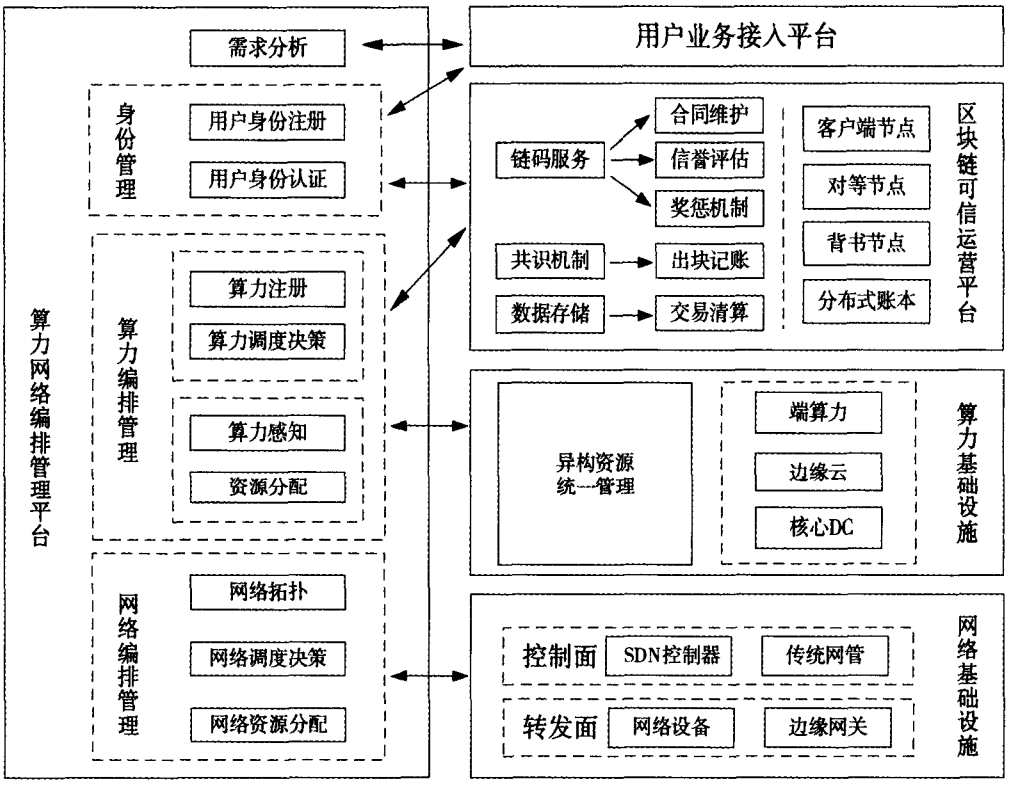

图 1　基于区块链的算力网络架构

在提出的架构中,典型的任务处理流程如下。用户提交注册请求并获得算力网络准入资格后,可在算力网络中请求和提供服务。算力网络消费方向算力网络编排管理平台发送服务请求,请求中包括对算力、网络连接、价格的要求,以及对算力服务的信誉要求等;编排管理平台对用户请求进行需求分析,选择匹配的算力服务调度策略,进行算力服务调度决策并将决策告知算力消费方和提供方;待算力消费方、提供方签订交易合约后,编排管理平台将通过算力网络控制面调度算力资源、建立网络连接,并持续监控合约的履行过程;计算任务结束后,由可信运营平台完成交易费用清算与算力服务信誉值更新。

3 基于区块链的算力网络信任评估与保障方案设计

在上节所提架构基础上,本节将进行基于区块链的算力网络信任评估与保障方案设计,本方案包括用户身份注册机制、算力服务注册机制、算力网络交易机制、算力网络信誉评估机制。

3.1 基于区块链的算力网络用户身份注册机制

为保障服务请求发起者的可信性,本节将首先提出基于区块链的算力网络用户身份注册机制。

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。

算力网络用户注册流程如图 2 所示。具体描述如下:

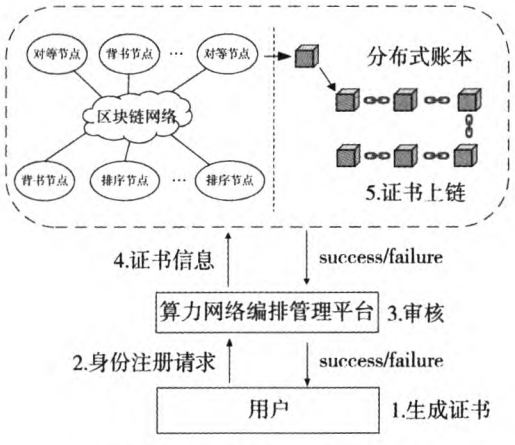

图 2 算力网络用户注册流程

(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。

(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。

(3) 算力网络编排管理平台收集用户的身份注册请求,根据用户提交的信息验证证书的合法性,最终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。

(4) 若判定成功,则将用户证书以"标识-证书-证书状态"的形式发送给区块链可信运营平台中的任一区块链节点。若失败,则向用户返回注册失败信息。

(5) 区块链节点接收到用户证书上链请求,经智能合约执行、背书节点验证和背书签名后,再由排序节点将收集到的交易分别进行排序,组装成区块后广播至网络中,全网节点接收区块后进行内容的验证,验证通过后更新分布式账本。

(6) 可信运营平台完成证书上链操作后,向编排管理平台返回注册成功信息;随后,编排管理平台向用户通告身份注册成功信息。

3.2 基于区块链的算力服务注册机制

为保障算力资源的可信接入,本节将设计基于区块链的算力服务注册机制。算力网络算力服务注册流程如图 3 所示。具体描述如下:

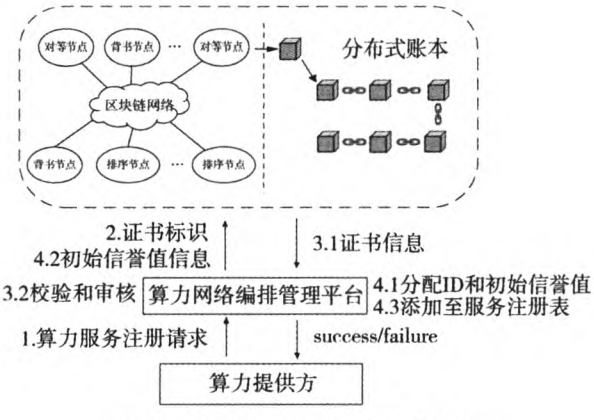

图 3 算力网络算力服务注册流程

(1) 算力提供方完成用户身份注册后,仍需进行算力服务注册请求。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。

(2) 算力网络编排管理平台接收到算力服务注册请求后,调用智能合约,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。

(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。若未通过证书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。

(4) 若算力服务审核通过,则顺序进行以下操作:①根据算力服务注册信息为算力服务分配服务 ID 并给定服务的初始信誉值;②将算力服务信息以"标识-服务 ID-初始信誉值"的形式发送给区块链节点,完成链上存储;③将算力服务信息存储至算力服务注册表中,算力服务注册表应包含服务 ID、服务 IP 和计算负载信息(计算能力、价格、计算时延等);④向用户返回算力服务注册成功信息。

3.3　基于区块链的算力网络交易机制

为达成算力网络可信交易,本节将提出基于区块链的算力网络交易机制。算力网络交易流程如图 4 所示。具体描述如下:

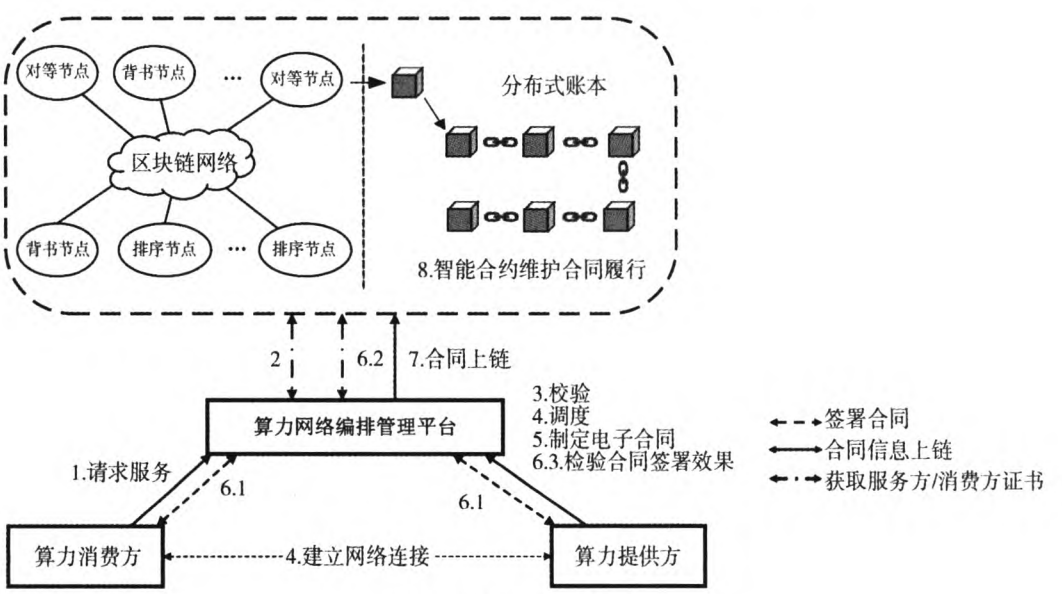

图 4　算力网络交易流程

(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。

(2) 算力网络编排管理平台接收到该服务请求后,调用智能合约根据证书标识向区块链节点查询消费方的证书信息。

(3) 获取消费方的证书信息后,算力网络编排管理平台对数字资质证书信息的合法性、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。

(4) 消费方身份信息验证通过后,算力网络编排管理平台将依据服务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。

(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、算力服务性能指标(例如可容忍的网络时延、算力、计算时间波动范围以及预期计算效果等)、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。

(6) 算力网络编排管理平台生成服务电子合同后,将合同依次发送给消费方以及提供方,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节点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。

(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。

(8) 通过区块链智能合约依据服务电子合同维护交易过程,交易过程维护包括:交易过程中,监管机构定时监测合同中的算力服务性能指标以及服务完成度等,并在交易结束时生成服务监测报告。交易结束后,①智能合约根据合同内的计费标准进行交易清算和资费转移;②监管机构将服务监测报告发送至区块链节点,存储在分布式账本中,智能合约将根据合同内的指标信息与服务监测报告对服务进行自动化评分,并将所得评分上链;同时消费方也对本次交易做出评价,并完成评价分数的链上存储;最终根据下文中的基于遗忘因子的时变信誉值计算方法计算和更新该算力服务的信誉值。

3.4 基于区块链的算力网络信誉评估机制

尽管区块链本身的技术特性可保证数据的不可篡改、可追溯,但它自身无法解决与数据有关的信任问题,所以仍需设计。文献[17]融合信誉系统,在物联网场景下设计了基于区块链的安全信任管理系统,但其提出的信誉评估方式并不适用于算力网络场景。本节在当前的研究基础上,针对算力网络场景,借助区块链智能合约技术,设计了适用于算力网络交易与评价机制的信誉评估方法:根据历史交易评价分数计算算力服务的信誉值。算力服务的信誉值可作为算力网络系统调度决策的重要考虑因素。下面,将首先描述单次交易的评价方法,随后在此基础处上提出基于遗忘因子的时变信誉值计算方法。

(1) 单次交易评价分数

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

首先,用户评价因素集合可表示为 $D=\{d_1,d_2,d_3,\cdots,d_n\}$ (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 $W=\{w_1,w_2,w_3,\cdots,w_n\}$,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 $u_1,u_2,\cdots,u_6$ 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,所对应的量化值分别为 0,0.2,0.4,0.6,0.8,1.0。若用户对交易因素的评级为 $R=\{r_1,r_2,r_3,\cdots,r_n \mid r_n \in U\}$,则用户对一次交易的评价分数可表示为

$$E_{\text{trader}} = W * R = (s_1, s_2, \cdots, s_n)$$

另外,每当交易完成时,智能合约根据电子合同规定的指标信息与服务监测报告对服务进行自动化评分,得到评价分数 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可表示为

$$E_{\text{seller}}(t) = \alpha_1 E_{\text{trader}} r(t) + \alpha_2 E_{\text{reg}}(t) \quad \alpha_1 + \alpha_2 = 1$$

其中,α_1、α_2 为评价分量的权重因子。当 $E_{\text{trader}}(t)$ 与 $E_{\text{reg}}(t)$ 相差较大时,需通过智能合约查询该用户前序服务评分情况,发现用户存在持续异常评分,则降低用户评分的权重值。

(2) 基于遗忘因子的时变信誉值计算方法

基于 Collard 等[19]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。

由上述单次交易评价分数的介绍中可知,提供方在 t_0 至 t_n 时间内,所完成的每笔交易的评价分数可表示为 $E_{\text{seller}}(t_0), E_{\text{seller}}(t_1), \cdots, E_{\text{seller}}(t_n)$,将这些评价分数加权累加即可得到算力服务在 t_n 时刻的信誉值 $R(t_n)$,可表示为

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

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。$\beta(t)$ 应是随时间增大而衰减的函数,例如 $\beta(t) = e^{-f(t)}$。

至此,本文在所提架构基础上,提出了基于区块链的算力网络信任评估与保障方案,分别为算力网络中的用户注册、算力服务注册、交易、信誉评估过程中所存在的安全可信问题提供解决方案。

4 实验验证

由于区块链技术的特性,本方案中链上存储信息天然具有防篡改和可追溯的特性。另外,作为实验验证,本节对本文所提出的方案进行编码实现和安全性评估。

利用 Hyperledger Fabric 搭建区块链实验环境,部署 4Peer+1Order 的区块链网络,采用实用拜占庭(Practical Byzantine Fault Tolerance, PBFT)共识算法。根据第 3 节方案设计所提出的算力网络注册、交易、信誉评估等机制,使用 Golang 编写智能合约,进而使用 Fabric-SDK 构建区块链信息流,包括:(1) 数据流。用于存储证书、算力服务信息、交易记录等。(2) 访问流。提供分布式账本存储信息的访问功能。(3) 计算流。用于计算单次交易评价分数,计算并更新算力服务的信誉值,进行交易清算和

资费转移等,设置初始 $\alpha_1 = \alpha_2 = 0.5$。

另外,搭建包含算力网络编排管理平台、资源提供方、资源消费方的算力网络实验环境,设置资源提供方的个数为 20 个(每个资源提供方提供 2~3 个算力服务),资源消费方的个数为 50 个;资源提供方初始信誉值为 70;资源消费方以及监管机构针对某次交易的评分范围为 0~100。

算力网络实验环境可通过 Fabric-SDK 与区块链环境交互,构成融合区块链的算力网络实验环境;若不接入上述区块链环境,则算力服务信誉值计算方式采用历史交易用户评分的平均值。下面将分别在融合区块链的算力网络环境和未接入区块链的算力网络环境中,对以下两种攻击进行实验。

(1) 共谋攻击

共谋攻击为恶意节点通过提供虚假的建议来破坏其他行为良好的用户的声誉,从而降低它们的信誉值。如图 5 所示,在未遭受共谋攻击情况下,假定算力提供方服务质量较高,设置全部消费方给予该算力服务正面评价,0~500 s 内信誉值从 70 逐渐升至 85。另外,分别在两种环境下进行共谋攻击实验:100 s 时,与无共谋攻击时相比,设置 50%的算力服务消费方对算力服务进行恶意评分,并设置每监测到消费方连续 3 次异常评分后,将 α_1 减半。实验结束时,算力网络实验环境中的算力服务信誉值由 79 逐渐降低至 55,融合区块链的算力网络实验环境中信誉值维持在 80。对比分析无共谋攻击情况下的信誉值变化与共谋攻击下的两条信誉值变化曲线,证明本方案对共谋攻击下的算力服务信誉值拥有良好的修正效果。

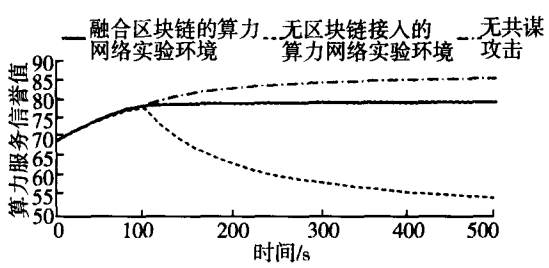

图 5　共谋攻击仿真结果

(2) 选票填充攻击

与共谋攻击相反,选票填充攻击中的恶意节点通过提供针对其他节点的良好意见来促进其他节点被信任的机会,类似于选举中的选票填充作弊行为。如图 6 所示,在无选票填充攻击情况下,设定算力服务信誉值维持在 70 至 75 之间。100 s 后,分别在融合区块链的算力网络实验环境和无区块链接入的算力网络环境中进行选票填充攻击实验:与无选票填充攻击时相比,设置 50%的消费方对算力服务进行作弊评分,以提高其信誉值。实验过程中,每监测到消费方连续 3 次异常评分后,将 α_1 减半。实验结束时,算力网络实验环境中的算力服务信誉值由 72 升至 90,融合区块链的算力网络实验环境中信誉值仍维持在 75 左右。对比分析 3 条信誉值变化曲线,证明本方案在应对选票填充攻击时,具有较好的弹性。

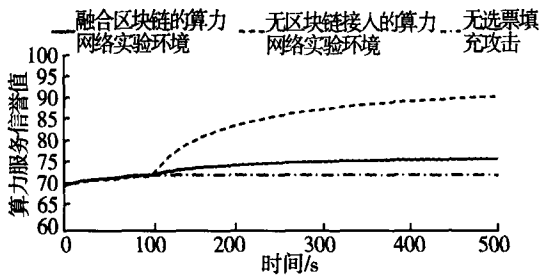

图 6　选票填充攻击仿真结果

在本节中,评估了应对攻击时本文所提方案的性能。仿真实验结果表明,与无区块链接入算力网络方案相比,本文所提出的融合区块链的算力网络信任评估与保障方案对共谋攻击、选票填充攻击提供了更高的弹性。

5　结束语

为了满足未来社会对信息处理的巨大算力需求和应对算网融合的发展趋势,业界提出了“算力网络”这一新兴网络架构和资源整合方案。然而算力网络的发展正处于起步阶段,少有学者对算力网络中的安全可信问题展开研究。本文归纳了算力网络中存在且尚未解决的安全可信问题,并借助区块链技术,提出了融合区块链的算力网络新型架构;在此架构基础上,设计实现了算力网络用户身份注册机制、算力服务注册机制、交易机制、信誉评估机制。最后,对本文所提方案进行安全性能评估,方案在应对共谋攻击、选票填充攻击时表现出了较好的弹性,为算力网络的算力资源共享提供安全可信保障。

参考文献:

[1] PHAM Q V, FANG F, HA V N, et al. A survey of multi-access edge computing in 5G and beyond: fundamentals, technology integration, and state-of-the-art[J]. IEEE Access, 2020, 8: 116974-117017.

[2] 于清林.从边缘计算到算力网络[J].产业科技创新,2020,2(3):49-51.

[3] LETAIEF K B, CHEN W, SHI Y M, et al. The roadmap to 6G: AI empowered wireless networks[J]. IEEE Com-

munications Magazine, 2019, 57(8): 84-90.

[4] 中国移动通信有限公司研究院.算力感知网络技术白皮书[EB/OL].[2020-11-10].http://www.idcquan.com/Special/ESIS2019.

[5] 中国联通网络技术研究院.中国联通算力网络白皮书[EB/OL].[2020-11-10].http://www.impcia.net/Uploads/report/2020-04-29/5ea92239af1e4.pdf, 2019.

[6] 雷波,刘增义,王旭亮,等.基于云、网、边融合的边缘计算新方案:算力网络[J].电信科学,2019,35(9):44-51.
LEI Bo, LIU Zengyi, WANG Xuliang, et al. Computing network: a new multi-access edge computing[J]. Telecommunications Science, 2019, 35(9): 44-51.(in Chinese)

[7] 曾诗钦,霍如,黄韬,等.区块链技术研究综述:原理、进展与应用[J].通信学报,2020,41(1):134-151.
ZENG Shiqin, HUO Ru, HUANG Tao, et al. Survey of blockchain: principle, progress and application [J]. Journal on Communications, 2020, 41(1): 134-151.(in Chinese)

[8] 中国信息通信研究院.区块链白皮书(2019 年)[EB/OL].[2020-11-12].http://www.caict.ac.cn/kxyj/qwfb/bps/201911/P020191108365460712077.pdf, 2019.

[9] LAHBIB A, TOUMI K, ELLEUCH S, et al. Link reliable and trust aware RPL routing protocol for Internet of Things [C] // IEEE 16th International Symposium on Network Computing and Applications (NCA). 2017: 1-5.

[10] WANG Y, VASSILEVA J. Trust and reputation model in peer-to-peer networks[C] // Proceedings 3rd International Conference on Peer-to-Peer Computing (P2P). 2003: 150-157.

[11] 邓晓衡,关培源,万志文,等.基于综合信任的边缘计算资源协同研究[J].计算机研究与发展,2018,55(3):449-477.
DENG Xiaoheng, GUAN Peiyuan, WAN Zhiwen, et al. Integrated trust based resource cooperation in edge computing[J]. Journal of Computer Research and Development, 2018, 55(3): 449-477.(in Chinese)

[12] DENNIS R, OWEN G. Rep on the block: a next generation reputation system based on the blockchain[C] // 10th International Conference for Internet Technology and Secured Transactions (ICITST). 2015: 131-138.

[13] PAN J L, WANG J Y, HESTER A, et al. EdgeChain: an edge-IoT framework and prototype based on blockchain and smart contracts[J]. IEEE Internet of Things Journal, 2019, 6(3): 4719-4732.

[14] KANG J W, YU R, HUANG X M, et al. Blockchain for secure and efficient data sharing in vehicular edge computing and networks[J]. IEEE Internet of Things Journal, 2019, 6(3): 4660-4670.

[15] KHAQQI K N, SIKORSKI J J, HADINOTO K, et al. Incorporating seller/buyer reputation-based system in blockchain-enabled emission trading application[J]. Applied Energy, 2018, 209: 8-19.

[16] CHEN I R, GUO J, BAO F Y. Trust management for SOA-based IoT and its application to service composition [J]. IEEE Transactions on Services Computing, 2016, 9(3): 482-495.

[17] MALIK S, DEDEOGLU V, KANHERE S S, et al. TrustChain: trust management in blockchain and IoT supported supply chains[C] // IEEE International Conference on Blockchain. 2019: 184-193.

[18] MOINET A, DARTIES B, BARIL J L. Blockchain based trust & authentication for decentralized sensor networks [EB/OL].[2020-11-12].https://arxiv.org/abs/1706.01730.

[19] COLLARD D, GAMBETTA D. Trust: making and breaking cooperative relations[J]. The Economic Journal, 1989, 99(394): 201.