

基于信任度评估的分布式算力交易方案

王英晓春^{1,2}, 王连海^{1,2}, 徐淑奖^{1,2}, 张淑慧^{1,2}, 刘天瑞^{1,2}

(1. 齐鲁工业大学(山东省科学院), 山东省计算中心(国家超级计算济南中心),

算力互联网与信息安全教育部重点实验室, 山东 济南 250014;

2. 山东省工业网络和信息网络安全重点实验室, 山东省基础科学研究中心(计算机科学), 山东 济南 250014)

摘要: 算力网络主要通过连接和整合分布式的异构计算节点, 实现网络和计算资源的优化及高效利用。在算力网络中, 节点因自身资源受限, 通常需要以交易形式请求其他节点的计算资源来完成计算任务, 引入信任度评估机制可以有效解决泛在异构节点所引起的节点可信度不高问题。然而, 现有的算力交易方案虽然将信誉作为选择交易方的重要依据, 但通常会选择信誉最高的节点, 导致新加入节点在算力交易中无法享有公平参与交易的机会, 且由于交易环境不可信, 节点很难评估交易反馈的可信度。为了解决上述问题, 提出了基于信任度评估的分布式算力交易方案, 通过智能合约对满足算力需求的计算节点实施自动化的信任度评估, 生成信任度降序列表, 基于随机选择算法从信任度高于一定阈值的节点中选定交易方, 以保证资源选择的随机性, 有效防止合谋攻击。同时, 利用适应性函数动态调整直接信任和间接信任的权重, 以跟踪计算节点的行为变化。此外, 借助区块链技术, 设计了一种衡量反馈可靠性的方法, 以减少因不可信节点提交恶意评分所造成的评估结果偏差。最后, 通过实验证明了所提方案在识别恶意评分和降低恶意行为影响方面的有效性。

关键词: 算力网络; 区块链; 信任度评估; 算力交易

中图分类号: TP393

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2025008

Distributed computing power trading scheme based on trustworthiness assessment

WANG Yingxiaochun^{1,2}, WANG Lianhai^{1,2}, XU Shujiang^{1,2}, ZHANG Shuhui^{1,2}, LIU Tianrui^{1,2}

1. Key Laboratory of Computing Power Network and Information Security, Ministry of Education, Shandong Computer Science Center

收稿日期: 2024-03-28; 修回日期: 2024-09-26

通信作者: 王连海, wanglh@sdas.org

基金项目: 国家自然科学基金(62102209); 国家重点研发计划(2023YFC3304903); 济南市“新高校20条”项目(202228017); 泰山学者工程(tsqn202312231); 山东省自然科学基金(ZR2024MF104, ZR2023QF129); 齐鲁工业大学(山东省科学院)科教产教融合试点工程重大创新类项目(2024ZDZX08); 齐鲁工业大学(山东省科学院)人才项目(2023RCKY144)

Foundation Items: The Natural Science Foundation of China (62102209), The National Key Research and Development Program of China (2023YFC3304903), The New 20 Project of Higher Education of Jinan, China (202228017), Taishan Scholars Program (tsqn202312231), Natural Science Foundation of Shandong Provincial (ZR2024MF104, ZR2023QF129), The Pilot Project for Integrated Innovation of Science, Education, and Industry of Qilu University of Technology (Shandong Academy of Sciences) (2024ZDZX08), Talent Project of Qilu University of Technology (Shandong Academy of Sciences) (2023RCKY144)

引用格式: 王英晓春, 王连海, 徐淑奖, 等. 基于信任度评估的分布式算力交易方案[J]. 网络与信息安全学报, 2025, 11(1): 79-91.

Citation Format: WANG Y X C, WANG L H, XU S J, et al. Distributed computing power trading scheme based on trustworthiness assessment[J]. Chinese Journal of Network and Information Security, 2025, 11(1): 79-91.

(National Supercomputer Center in Jinan), Qilu University of Technology (Shandong Academy of Sciences), Jinan 250014, China

2. Shandong Provincial Key Laboratory of Industrial Network and Information System Security,
Shandong Fundamental Research Center for Computer Science, Jinan 250014, China

Abstract: The computing power network was primarily designed to optimize and efficiently utilize network and computing resources by connecting and integrating distributed heterogeneous computing nodes. Within this network, nodes frequently required computing resources from other nodes through trading mechanisms due to their limited local resources. The introduction of a trust evaluation mechanism effectively addressed the issue of low trustworthiness among ubiquitous heterogeneous nodes. However, existing computing power trading schemes, which relied on reputation as a key criterion for selecting trading partners, typically favored nodes with the highest reputation. This approach resulted in newly joined nodes being unable to participate fairly in computing power trading, and the untrustworthy trading environment made it difficult for nodes to assess the credibility of trading feedback. To address these challenges, a distributed computing power trading scheme based on trust evaluation was proposed. In this scheme, the trust evaluation of computing nodes meeting the computing power requirements was automated through smart contracts, generating a trust list sorted in descending order. A random selection algorithm was utilized to choose trading partners from nodes with trust levels above a predefined threshold, ensuring randomness in resource selection and effectively mitigating collusion attacks. Additionally, an adaptive function was employed to dynamically adjust the weights of direct and indirect trust, enabling the tracking of behavioral changes in computing nodes. Furthermore, a method for measuring feedback reliability was designed using blockchain technology to reduce the bias in evaluation results caused by untrustworthy nodes submitting malicious ratings. Finally, experimental results demonstrated that the proposed scheme effectively identified malicious ratings and reduced the impact of malicious behaviors. The scheme is shown to ensure fair participation in trading for newly joined nodes while enhancing the reliability of trading feedback.

Keywords: computing power network, blockchain, trust worthiness evaluation, computing power trading

0 引言

随着物联网、云计算、边缘计算^[1]的快速发展,计算资源的部署逐步趋于泛在化,与此同时,新兴业务的不断兴起和发展,对计算资源的需求急剧攀升,因此,如何高效协同地利用这些泛在计算资源成为当前网络研究的一项重要课题。在此背景下,算力网络的概念被提出^[2]。算力网络通过网络连接来整合分布式的计算资源,为用户提供高效、可靠的算力服务,提高算力资源的利用率。算力网络中的节点可以通过买卖、租赁方式共享计算资源,计算资源的拥有者可以将其闲置的计算资源出租或出售,而计算资源的请求者可以购买这些资源来完成自己的计算任务,从而实现资源的优化利用,算力交易的雏形由此显现。

算力交易虽然为节点提供了灵活、经济、高效的计算资源获取方式,但仍然面临严峻挑战。一方面,由于算力网络中的计算资源来源于不同的所有者,包括云服务器、边缘服务器、智能终端设备等,节点的异构性和泛在性对算力交易的安全造成

严重威胁。另一方面,现有的算力交易方案虽然将信誉作为交易方的选择依据之一,但计算资源在性能和服务质量方面存在差异,通过单次交易的评价难以全面反映节点的信任度。因此,算力交易面临着严峻的信任问题,需要对交易双方进行有效的信任管理,以确保交易的安全、稳定。

信任管理(TM, trust management)作为控制和维护信任的有效手段^[3],能够帮助用户判断提供计算资源的节点是否可信,也为算力交易平台提供了对交易参与方的奖惩依据。然而,存在恶意节点试图伪造信任信息,破坏评估过程,因此,如何保证信任度评估结果的安全性和不易篡改成为实现可靠评估的关键。另外,传统集中式的算力交易模式在资源管理、网络延迟、安全性等方面也存在显著问题。

区块链作为一种分布式、去中心化的账本技术,开创了一种在不可信的竞争环境中低成本建立信任的新型计算范式和协作模式^[4],为信任评估提供了可行的高信任、低成本解决方案,使用

智能合约执行信任度评估可以有效避免评估过程被恶意操纵, 将信任信息上链存储, 能够提高信任度评估过程的透明度, 防止数据被篡改。同时, 区块链采用分布式数据结构, 可以安全地存储算力交易记录, 无须中心授权点^[5], 能够有效解决传统集中式交易模式存在的问题。此外, 算力网络的复杂性和计算资源的时变特性, 使得交易参与者可以在网络中扮演不同的角色, 既可以作为计算节点通过执行某个任务来获得相应的报酬, 又可以作为任务节点发布算力需求并支付报酬, 让其他计算节点来执行该计算任务。

基于上述分析, 本文提出一种基于信任度评估的分布式算力交易方案, 以解决算力网络中计算节点异构泛在特性导致的信任问题, 为算力交易构建一个安全可信的交易环境。本文主要贡献如下。

1) 设计了一种信任度评估模型, 采用基于反馈的直接信任和基于推荐的间接信任相结合的计算方法, 同时, 基于直接信任度的波动差异设计适应性函数, 自适应调整直接信任和间接信任的权重, 并根据区块链上存储的历史评分生成评分可信度, 聚合可信度来衡量反馈可靠性, 有效识别恶意评分和不可靠推荐。

2) 提出了一种基于信任度评估的分布式算力交易方案, 通过智能合约对满足算力需求的计算节点实施自动化的信任度评估, 生成信任度降序列表, 经过阈值筛选后, 基于随机选择算法从筛选后的节点中选定交易方, 以保证资源选择的随机性, 有效防止合谋攻击。

3) 对所提方案进行了安全性和性能分析, 证明所提方案在识别恶意评分和减小恶意行为影响方面的有效性。

1 相关工作

1.1 算力交易

算力网络是通过网络连接将计算资源合理配置到有需求的一方, 为了规范算力交易, Ren等^[6]提出了支持多重角色切换和利润均衡的算力交易框架。Lyu等^[7]提出了一种去中心化的算力资源交易机制。该机制使用区块链构建交易的整体框架, 利用智能合约执行交易流程, 保证流程的可信性, 同时设计了服务质量评分区块来记录用户对算力资源的服务评价。为了优化计算资源

配置和资源定价, Wu等^[8]构建了基于云挖掘机制的算力交易模型, 并将交易建模为Stackelberg博弈过程, 以实现利润最大化。Lin等^[9]提出了一种点对点计算资源交易系统, 用来有偿共享闲置计算资源, 同时, 构建了一个两阶段的Stackelberg博弈, 得出最优资源定价和交易量, 以平衡动态的计算需求。然而, 在5G时代计算节点下沉, 算力更加分散化, 如何保证算力交易的可信是亟须研究的问题^[10]。为此, 学者提出了多种解决方案, 在基于区块链的方案中, Zhang等^[11]提出一种在物联网区块链(BCoT)中可验证且保护隐私的云矿池选择方案, 以解决矿池间的信任问题。Kwantwi等^[12]提出一种基于分层区块链的切片间计算资源交易方案。Wang等^[13]提出了一种基于区块链的自私挖矿检测方案, 利用区块高度和区块交易记录特征, 实时检测网络中的自私挖矿行为。Wu等^[14]提出了一种云计算公平隐私支付方案BPF-Payment, 通过引入区块链以解决云计算中支付不公平问题, 同时采用Paillier同态加密方案让区块链直接验证数据, 保证数据的隐私性, 但因同态加密计算复杂度较高, 性能瓶颈限制了其广泛应用。因此, Li等^[15]提出使用基于信誉的支付方式, 以快速完成计算资源交易。Fan等^[16]提出了一种资源交易系统, 利用混合区块链和支付通道技术, 在请求者和边缘节点之间实现可信、快速、低成本和高频率的支付。Yu等^[17]提出一种矿工类型鉴别机制, 构造信誉管理模型对矿工的行为进行衡量, 有效识别恶意矿工。Cheng等^[18]提出了一种基于智能合约的可信资源分配机制, 利用声誉评估机制来评估边缘服务器服务质量。

综上所述, 目前算力交易各方面的研究并不完善, 同时, 算力网络的复杂性和计算资源的时变特性, 使得交易双方很难构建稳定的信任关系, 算力网络仍缺乏对算力资源设备的TM方案^[19]。本文将以交易者的选择为切入点, 旨在构建一个安全可信的算力交易环境。

1.2 信任管理

现有TM模型可分为集中式和分布式两类^[20]。

集中式TM是一种传统的信任模型, 依赖于中央权威机构管理和验证参与者之间的信任关

系, 信任信息的管理相对集中, 易于实现和维护。Saied 等^[21]设计了一个基于上下文感知的 TM 系统, 能够根据不同的上下文为合作节点动态分配信任值。Awan 等^[22]提出了一种基于基础设施的 NeuroTrust 方法, 由双方的服务器实行 TM, 同时利用众多参数生成信任值, 聚合信任值来实现不可抵赖性。集中式 TM 模型实现起来简单, 但存在单点故障和资源扩展性差等问题。为了解决这些问题, 分布式 TM 模型应运而生。

分布式 TM 是一种去中心化的信任模型, 不依赖于中央权威机构, 而是通过网络中多个节点之间的共识机制来管理和验证交易的信任关系, 解决了单点故障问题。Xiong 等^[23]提出了一个基于声誉的信任支持框架 PeerTrust, 用于量化交易反馈和评估同伴的可信度。Bhattacharjee 等^[24]提出了一种基于相对熵的信任评分模型, 使用信任评分对受损的智能电表与未受损的智能电表进行分类。Le 等^[25]结合动态距离算法提出了一种信任模型, 使 MEC 节点能够根据信任分数决定信息迁移点。Ren 等^[26]提出了一种多维信任评价机制, 利用不同网络实体观察后形成的不同意见综合评价物联网边缘设备的可信度。Moustafa 等^[27]提出了一种分散式声誉管理模型, 每个节点的声誉评估由自身及其邻居共同完成。

分布式 TM 模型虽然扩展性好, 但是未解决数据审计和一致性问题, 因此又引入了区块链技术, 以构建更加安全、透明的 TM 模型。Yang 等^[28]提出一种移动网络联邦学习方案, 该方案允许服务端利用主观逻辑模型对参与训练的移动任务发布者进行信誉评估。Huang 等^[29]提出了一种交易链和信誉链相结合的双链架构, 利用信誉验证节点之间的异质性, 还提出了基于声誉的分片和领导者选择方案。然而, 由于无法消除声誉计算中的主观性, 信任评估结果不准确。Al-khafajiy 等^[30]提出了一种基于雾计算环境的 TM 架构, 从服务质量和雾节点对计算过程的安全保护来综合评估雾节点的信任等级, 从而识别和隔离恶意的雾节点。Kouicem 等^[31]基于区块链提出了一种分层和可扩展的 TM 协议, 该协议使高度移动的物联网设备能够准确地评估和共享关于其他设备的信任建议。Liu 等^[32]基于隐马尔可夫模型提出了一种车辆信任

评估算法, 能够有效甄别恶意车辆和恶意路边单元 (RSU, road side unit)。Kudva 等^[33]基于区块链设计了一个去中心化的信任评分框架, 首先, 节点计算与之相邻节点的信任度, 由 RSU 汇总并验证所有节点的信任得分, 以检测 VANET 中的内部攻击者并将其列入黑名单。Liu 等^[34]提出了一种基于区块链的半集中式 TM 系统架构, 考虑了单域和多域两种环境下的信任评估, 通过聚合直接和间接信任信息, 计算出动态恶意设备的信任值。Du 等^[35]提出了一种基于联盟链和贝叶斯推理的 TM 方法, 以构建信息共享的可信环境。

综上所述, 基于区块链的 TM 机制解决了数据审计和一致性问题, 能够适应更加复杂的信任关系, 但信任评估方法还有待完善。

2 信任度评估模型

本文设计了一个信任度评估模型来评估计算节点的信任度, 为了使计算节点的信任度更加客观和准确, 模型包含直接信任度和间接信任度两部分。信任度评估模型如图 1 所示。在该模型描述中, i 表示任务节点, j 表示计算节点, 信任度参数的计算都在智能合约中执行。

2.1 直接信任度

在信任度评估模型中, 直接信任度是基于任务节点 i 与计算节点 j 直接交互而形成的信任, 由智能合约收集响应比、信任等级和交易表现指数计算得到, 并记录在区块链中。

(1) 响应比

响应比指计算节点 j 对任务节点 i 发布的算力请求的响应频率。根据式(1)计算任务节点 i 与计算节点 j 在 t 时刻的响应比。

$$RV_j^i(t) = \frac{RES_j^i(\Delta t)}{REQ_j^i(\Delta t)} \quad (1)$$

其中, $RES_j^i(\Delta t)$ 指计算节点 j 对任务节点 i 请求的响应次数, $REQ_j^i(\Delta t)$ 指任务节点 i 向计算节点 j 请求资源的总数。为了节省计算开销, 只考虑时间间隔 Δt 内发生的交互。

(2) 信任等级

信任等级表示任务节点 i 对计算节点 j 在直接交互中的信任程度, 这是通过双方历史交互中的服务评分来衡量的, 利用式(2)判断任务节点 i 在 t

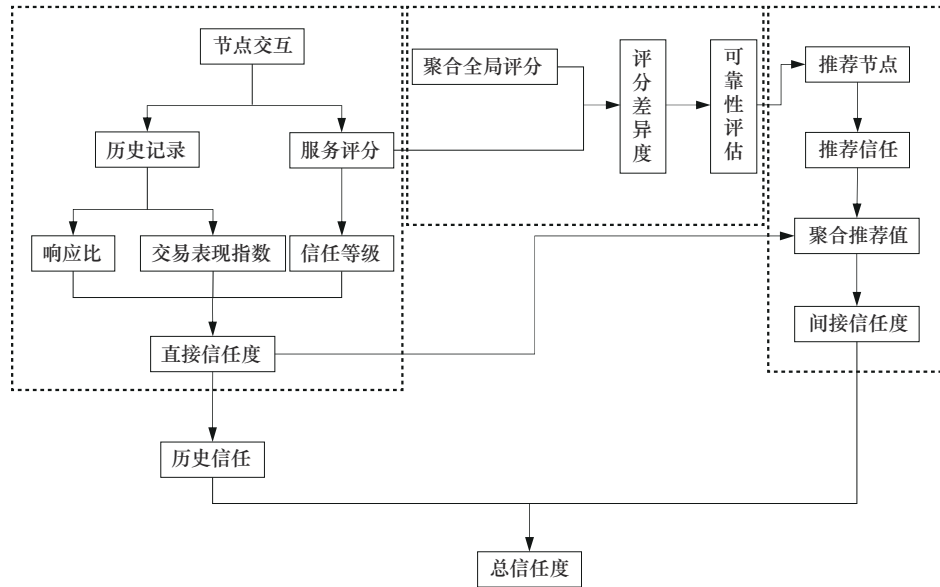


图1 信任度评估模型

Figure 1 Trustworthiness assessment model

时刻对计算节点 j 的信任等级。

$$TL_j^i(t) = \frac{\sum_{t \in \Delta t} \left(SR_j^i(t) \cdot e^{-\frac{\Delta t^2}{2\sigma^2}} \right)}{\sum_{t \in \Delta t} e^{-\frac{\Delta t^2}{2\sigma^2}}} \quad (2)$$

其中, $SR_j^i(t)$ 为任务节点 i 在 t 时刻对计算节点 j 的服务评分, $e^{-\frac{\Delta t^2}{2\sigma^2}}$ 表示评分的衰减度, σ 表示衰减速率。

(3) 基于历史数据的交易表现指数

对算力请求者来说, 历史交易的成功率也具有一定的参考价值。首先, 计算任务节点 i 与计算节点 j 成功交易的概率如式(3)所示。

$$Trap_j^i = \frac{\sum SR_j^i}{\sum_{k \in U} (SR_k^i)} \quad (3)$$

然后, 通过任务节点 i 对计算节点 j 的历史服务评分计算好评率, 设定服务评分在 0.8 分以上即为好评, 如式(4)所示。

$$Per_j^i = \frac{\sum_{SR_j^i \geq 0.8} (SR_j^i)}{\sum (SR_j^i)} \quad (4)$$

最后, 根据交易率和好评率计算出最终的交易表现指数, 如式(5)所示。

$$TPI_j^i = \frac{\omega_1 \cdot Trap_j^i + \omega_2 \cdot Per_j^i}{\omega_1 + \omega_2} \quad (5)$$

这里, ω_1 和 ω_2 分别表示交易率和好评率在交易表现指数中的比重。

任务节点 i 对计算节点 j 的直接信任度如式(6)所示。

$$DT_j^i(t) = RV_j^i(t) \times TL_j^i(t) \times TPI_j^i \quad (6)$$

2.2 间接信任度

个体的直接观察和历史经验可能会受到主观或其他因素的影响, 因此引入间接信任度来提高评估的客观性。

智能合约基于其他可信节点的推荐来评估任务节点 i 对计算节点 j 的间接信任度, 将其他可信节点在时间间隔内对计算节点 j 的直接信任度称为推荐, 提供推荐的任务节点构成了推荐者集合 $R = \{r_1, r_2, \dots, r_{\max}\}$, $r_{\max}$ 为推荐者的最大数量, 利用式(7)可以计算出间接信任度。

$$IT_j^i(t) = \frac{\sum_{k \in R} (DT_j^k(t) \times RT_k^i(t))}{\sum_{k \in R} (RT_k^i(t))} \quad (7)$$

其中, $DT_j^k(t)$ 为推荐者 k 在 t 时刻对计算节点 j 的直接信任度, $RT_k^i(t)$ 为任务节点 i 对推荐者 k 的推荐信任, 通过推荐者的服务评分可靠性来验证。为节省计算开销, 本方案只考虑不小于推荐信任阈值 $RT_{\text{threshold}}$ 的推荐, 以此过滤掉不可靠的推荐。

2.3 总信任度

总信任度表示任务节点 i 对计算节点 j 的综合

信任程度, 如式(8)所示。

$$TT_j^i(t) = \alpha_i \times DT_j^i(t) + \beta_i \times IT_j^i(t) \quad (8)$$

其中, α_i 为直接信任权重, β_i 为间接信任权重, 由适应性函数动态更新。

2.4 服务评分

在算力交易完成后, 任务节点 i 根据计算任务的结果、耗时、价格等返回一个主观评分, 算力交易平台会根据算力交易过程中的监测信息给出一个客观评分, 综合主观评分和客观评分得到本次交易的综合评分, 评分区间为 $[0 \sim 5]$, 5 代表非常满意, 0 代表非常不满意。

2.5 服务评分可靠性

服务评分可靠性表示节点所给出的服务评分的可信程度。由于服务评分是节点对交易服务的满意度, 具有高度主观性, 若缺少有效评估其可靠性的方法, 会对被评分节点的信任度产生不利影响。因此, 本文设计了评估服务评分可靠性的方法, 防止异常评分干扰信任度评估过程的准确性。

首先, 假设在 t 时刻, 任务节点 i 对计算节点 j 进行了一次服务评分, 记作 $SR_j^i(t)$ 。

然后, 智能合约汇总所有节点对计算节点 j 的评分来计算全局评分 $GR_j^U(t)$, 如式(9)所示。

$$GR_j^U(t) = \frac{\sum (\overline{SR_j^U(t)} \times \overline{TT_U(\Delta t)})}{\sum (\overline{TT_U(\Delta t)})} \quad (9)$$

其中, $(\overline{TT_U(\Delta t)})$ 表示所有评分节点在时间间隔 Δt 内的信任度平均值, 以信任度平均值作为服务评分的权重参与到全局评分的计算中。

计算服务评分可信度的方法如式(10)所示。

$$RC_j^i(t) = \frac{1}{|SR_j^i(t) - GR_j^U(t)| + 1} \quad (10)$$

最后, 通过汇总服务评分可信度来度量服务评分可靠性 $RD_i(t)$ 。

$$RD_i(t) = \frac{1}{|U|} \sum_{t \in \Delta t} RC_U^i(t) \quad (11)$$

2.6 适应性函数

为了动态调整信任度评估模型, 本文设计了一种基于波动率的适应性函数自适应地调整权重 α_i 和 β_i 的大小。波动率 Vol_i 是直接信任度变动程度的度量, 基于波动率调整 α_i 和 β_i 的大小, 能够根据直接交互的信任关系变化动态调整信任度评

估模型, 波动率 Vol_i 如式(12)所示。

$$Vol_i = \sqrt{\frac{\sum_{m=1}^n (DT_m - \overline{DT})^2}{n}} \quad (12)$$

其中, DT_m 是任务节点 i 对计算节点 j 的直接信任度集合中的第 m 个值, $\overline{DT}$ 是所有直接信任度的均值, n 是时间间隔内任务节点 i 和计算节点 j 直接交互的总数。

适应性函数如式(13)所示。

$$\begin{cases} \alpha_i = \alpha_{i-1} + k \cdot Vol_i \\ \beta_i = 1 - \alpha_i \end{cases} \quad (13)$$

式中, 任务节点 i 对计算节点 j 的直接信任度的波动率越大, α_i 随之增大, 直接信任度在整个评估过程中的权重也就越大, 相应地, β_i 将减小, 使得间接信任度在评估时被考虑的权重变小, 以更敏感地跟踪信任度的变化。当波动率较小时, α_i 和 β_i 将缓慢调整。通过不断地调整 α_i 和 β_i 的值, 能更好地跟踪交易双方信任关系的变化。

3 方案实现

3.1 系统模型

本文提出了一种基于信任度评估的分布式算力交易方案, 其系统架构如图2所示。

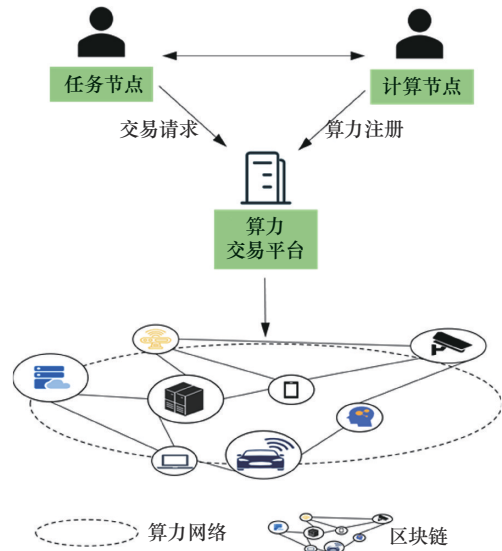


图2 系统架构
Figure 2 System architecture

角色主要包括计算节点和任务节点。角色的详细描述如下。

1) 计算节点。计算节点作为计算资源提供

者, 负责为任务节点提供算力资源。

2) 任务节点。任务节点作为任务发布者, 向计算节点发布计算资源请求, 并使用这些资源完成自己的计算任务。

本方案借助区块链技术构建可信的算力交易平台, 将算力交易的逻辑规则写入智能合约, 对算力交易进行监管。任务节点可以在交易平台浏览资源并提交相应的算力请求, 交易记录被存储在区块链中, 从而保证交易的透明性和不易篡改。

交易双方可以在任务节点和计算节点两种角色之间自由切换。所提方案鼓励计算节点提供高质量的计算资源, 计算节点的信任度会随其服务质量而更新。较高的信任度将有助于计算节点在交易过程中获得更多的报酬, 信任度低于一定阈值的计算节点将无法再进行算力交易。

表1列出了本文所使用的符号和定义。

3.2 交易流程

算力交易流程可以分为以下3个阶段。

表1 符号和定义

Table 1 Notations and definitions

符号	定义
U	任务节点集合
N	任务节点的数量
R	推荐者集合
D_i	任务节点 i 的算力资源需求
S	候选者集合
Δt	时间间隔
σ	衰减速率
DL	信任度降序列表
C_s	参与随机选择算法的候选者 s 的数量
$RES_j^i(\Delta t)$	计算节点 j 在 Δt 内响应任务节点 i 的次数
$REQ_j^i(\Delta t)$	任务节点 i 在 Δt 内向计算节点 j 请求资源的总数
$RV_j^i(t)$	任务节点 i 在 t 时刻对计算节点 j 的响应比
$SR_j^i(t)$	任务节点 i 在 t 时刻对计算节点 j 的服务评分
$TL_j^i(t)$	任务节点 i 在 t 时刻对计算节点 j 的信任等级
$Trap_j^i$	任务节点 i 与计算节点 j 的交易率
Per_j^i	任务节点 i 对计算节点 j 的好评率
TPI_j^i	任务节点 i 对计算节点 j 的交易表现指数
$DT_j^i(t)$	任务节点 i 在 t 时刻对计算节点 j 的直接信任度
$RT_k^i(t)$	任务节点 i 在 t 时刻对推荐者 k 的推荐信任
$RC_j^i(t)$	任务节点 i 在 t 时刻对计算节点 j 的评分可信度
$RD_i(t)$	任务节点 i 在 t 时刻的评分可靠性
$IT_j^i(t)$	任务节点 i 在 t 时刻对计算节点 j 的间接信任度
$RT_{threshold}$	推荐信任阈值
r_{max}	推荐者的最大数量
$GR_j^U(t)$	聚合 U 中所有任务节点在 t 时刻对计算节点 j 的评分形成的全局评分
Vol_t	直接信任度在 t 时刻的波动率
α_t	直接信任度在 t 时刻所占权重
β_t	间接信任度在 t 时刻所占权重
$TT_j^i(t)$	任务节点 i 在 t 时刻对计算节点 j 的总信任度

阶段 1: 准备阶段。所有节点在区块链中完成身份注册后, 计算节点还需进行算力注册, 并实时更新空闲算力, 这里任务节点集合定义为 $U = \{1, 2, \dots, N\}$, N 为任务节点的数量。任务节点 $i \in U$ 则可以在算力交易平台浏览算力资源并发布自己的算力资源需求 D_i , 智能合约与任务节点交互完成订单确认后, 算力交易平台通知所有已进行算力注册且满足算力资源需求的计算节点响应应该请求。

阶段 2: 交易阶段。计算节点收到通知后, 考虑成本、时间开销等因素, 并通过发送响应消息表示愿意提供计算资源, 所有响应的计算节点构成了交易候选者集合 S 。为确保 TM 的安全性和可信性, 信任度计算逻辑被写入智能合约, 由智能合约计算和更新所有候选者 $s \in S$ (候选者为潜在的为任务节点提供计算资源的计算节点) 的信任度, 生成信任度降序列表, 并自动完成交易双方的匹配。算法 1 给出了基于智能合约的信任度评估算法。首先, 智能合约计算任务节点与计算节点之间的响应比 $RV_j^i(t)$ 和信任等级 $TL_j^i(t)$, 然后统计历史交易率 $Trap_j^i$ 和好评率 Per_j^i , 最后智能合约根据式(6)得到计算节点的直接信任度 $DT_j^i(t)$ 。其次, 智能合约需要统计所有与计算节点有历史交互的任务节点对其的直接信任度, 并以该任务节点自身评分可靠性为权重, 基于式(7)获得计算节点的间接信任度 $IT_j^i(t)$ 。智能合约结合 $DT_j^i(t)$ 和 $IT_j^i(t)$, 并根据直接信任度的波动率赋予二者权重, 计算和更新计算节点的总信任度 $TT_j^i(t)$ 。具体的信任度评估方法如第 2 节所述。最后, 基于随机选择算法从信任度高于一定阈值的节点中选定交易方, 并将结果返回给任务节点。

算法 1 基于智能合约的信任度评估算法

输入 $U, S, R, i, j, k, SR_j^i(t)$
 输出 计算节点的总信任度 $TT_j^i(t)$
 1) if j 向 i 提供资源 then
 2) i 将评分 $SR_j^i(t)$ 提交给智能合约;
 3) 根据式(10)计算 i 的评分可信度;
 4) 根据式(11)计算 i 的评分可靠性;
 5) end if

6) for i in U do

7) if j in S then

8) 根据式(6)计算直接信任度;

9) if k in R and k 与 j 有历史交互 then

10) 统计 k 对 j 的直接信任度, 获取 k 的评分可靠性;

11) 根据式(7)计算间接信任度;

12) end if

13) end if

14) 根据式(8)计算节点的总信任度;

15) end for

16) return $TT_j^i(t)$

算力交易平台拟定电子合同并提供给双方进行签订, 双方签订合同后用各自的私钥进行签名。为缓解区块链的存储压力, 电子合同使用线下数据库存储, 只将电子合同的 Hash 值上链存储。最后, 只有在任务节点向智能合约转存不低于资源成本的比特币作为报酬后, 算力交易平台才会通知计算节点向任务节点提供计算资源。

阶段 3: 反馈和结算阶段。完成计算任务后, 任务节点释放资源, 并根据结果、耗时、价格等指标对本次交易进行评分。智能合约收集当前计算节点的所有历史评分, 并计算当前任务节点对计算节点的评分与所有历史评分的偏差以获得此任务节点的评分可信度 $RC_j^i(t)$, 聚合固定时间间隔内的评分可信度, 生成该任务节点的评分可靠性, 将此评分及其可靠性值上链存储, 作为下一次评估该计算节点信任度的依据之一。算力交易平台通过比较 Hash 值完成校验, 防止合同被篡改带来的交易纠纷, 算力交易平台自动完成结算, 算力交易结束。算力交易过程由算法 2 描述。

算法 2 基于信任度评估的分布式算力交易算法

输入 $TT_j^i(t)$

1) for 任务节点 $i \in U$ do

2) 提交算力需求 D_i ;

3) end for

4) for $s \in S$ do

5) 计算每个候选者总信任度分数 $TT_j^i(t)$, 并降序排列生成信任度降序列表 DL;

- 6) 从列表中自上而下选择 C_s 个节点；
 - 7) 调用随机选择算法选定计算节点交易；
 - 8) **end for**
- 算力交易流程如图3所示。

4 方案分析

4.1 安全性分析

(1) 防止合谋攻击

合谋攻击指两个或多个节点协同行动，以达成共同的恶意目的，获取不正当利益。如果节点之间合谋，可能通过操纵信息或者隐藏真实行为来提高彼此的信任度，导致系统的信任度分配失衡，一些不诚实的节点获得过多的交易机会，牟取不正当报酬。所提方案会对每次交易的服务评分进行筛选，只有评分可靠性高于一定阈值的评分才会被存储到区块链中，并用于下一轮的信任度评估，同时，评分可靠性低于阈值的评分行为会被记录在信任数据中，并对评分源节点的信任度产生影响，通过评分可靠性发现串通节点和恶意行为证据，并对合谋节点采取惩罚措施，合谋节点只有通过后续的诚实行为提高评分可靠性，才能重新进入算力交易。此外，通过随机选择策略，增加交易方选择的随机性，有效防止合谋攻击。最后，交易记录和信任评估过程以及相关信任信息被保存在区块链中，确保评估的准确性和透明性。

(2) 识别恶意服务

恶意服务指在算力交易过程中，计算节点表现出与以往行为差异较大的活动。一方面，利用

区块链可以监测计算节点的信任度变化趋势，如果监测到突然的信任度变动，就可以通过信任度识别潜在的恶意服务节点；另一方面，节点反馈评分的整体降低也能说明计算节点的自主性动态服务行为的异常，为识别恶意服务节点提供依据。

(3) 防止恶意评分

恶意评分指任务节点试图用一个不真实的服务评分干扰对计算节点的信任度评估过程。常见的方式有两种：一种是内部合谋，节点之间相互操纵服务评分，试图破坏信任评估过程的可信度和准确性；另一种是外部合谋，共同陷害诚实节点。因此，必须确保服务评分的可靠性。本方案通过检查任务节点所给出的服务评分与整个服务评分集合的偏差来计算其可靠性，从而识别出恶意评分节点，保证计算节点能够获得客观、准确的评价。同时，与任务节点合谋的计算节点，其信任度也会随之下降，只有通过更多的正向交互才能再次提高信任度。信任度越低，表明在过去交易中的表现越差，该节点将逐渐被淡化出交易。由上可证明所提出的信任度评估模型可有效防止恶意评分。

4.2 性能分析

4.2.1 实验设置

实验在配置为Intel CPU i9-13900HX处理器、16 GB内存、操作系统为Windows 11的计算机上进行，并基于Netlogo6.4.0来评估信任度评估模型的性能，Netlogo是用来对自然和社会现象进行仿真的可编程建模环境。另外，使用以太坊来模拟区块链环境，在Remix IDE环境中采用Solidity

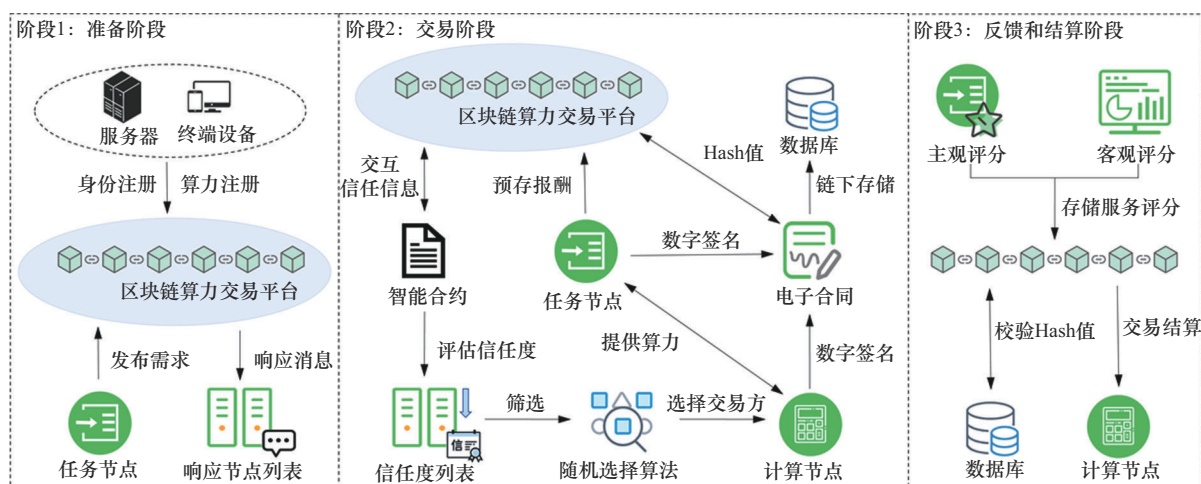


图3 算力交易流程

Figure 3 Computing power trading process

语言编写智能合约并部署到以太坊上。

在 Netlogo 仿真实验中, 设置 10 个任务节点、10 个计算节点。考虑有恶意服务和恶意评分两种类型的恶意行为。恶意服务是指部分计算节点在提供算力资源过程中存在不诚实行为, 企图破坏算力交易。恶意评分是指部分任务节点提供不真实的服务评分, 企图扰乱信任评估的准确性。

4.2.2 动态服务行为的信任度评估

本实验主要关注信任度评估模型在捕捉计算节点行为变化方面的敏感性。首先维持计算节点的行为不变, 观察诚实的任务节点对计算节点的信任度变化。动态服务行为的信任度评估如图 4 所示, 可以观察到 5 个任务节点对计算节点的信任度的曲线走势基本一致, 且均保持在较高的水平。经过大约 60 次的交互模拟后, 将计算节点的行为从诚实行为改为恶意行为。如图 4 所示, 5 个任务节点对计算节点的信任度产生明显下降, 但 5 条曲线的变化趋势仍然一致, 表明所提出的信任度评估模型对不诚实行为的反应迅速, 可以有效检测出恶意服务行为。

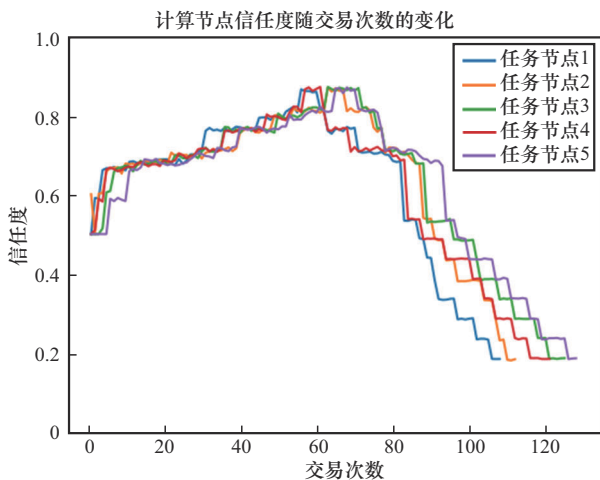


图 4 动态服务行为的信任度评估

Figure 4 Trust assessment of dynamic service behavior

4.2.3 服务评分可靠性评估

本实验证明了服务评分可靠性的计算方法在信任度评估模型中的优势。服务评分可靠性随行为的变化如图 5 所示。首先, 任务节点一直提供真实评分, 在完成第 30 次交易后开始提供恶意评分, 其服务评分可靠性产生相对显著的波动, 服务评分可靠性的降低会导致恶意评分在间接信任度评估中较少

或不被考虑。因此, 所提出的服务评分可靠性可以有效识别恶意评分。此外, 评分记录在区块链上, 区块链的去中心化和不易篡改性能够有效抵御内部攻击, 使计算出的信任度更加可靠。

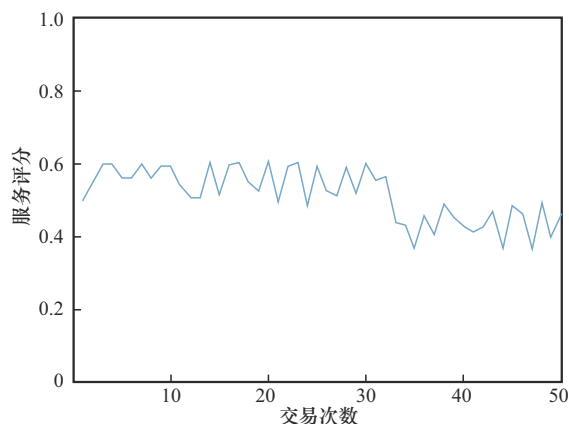


图 5 服务评分可靠性随行为的变化

Figure 5 Change in service score reliability with behavior

4.2.4 节点整体信任度分布

本实验选定一个计算节点, 查看其在某一时刻的信任度分布。实验结果如图 6 所示, 横坐标代表某一时刻与之交互的任务节点, 纵坐标代表任务节点对此计算节点的信任度, 从图中可以看出, 此节点在历史交互中的诚实行为受到整个网络中与之交互过的其他节点的普遍认同, 具体表现为各节点对该节点的信任度相近或相等。

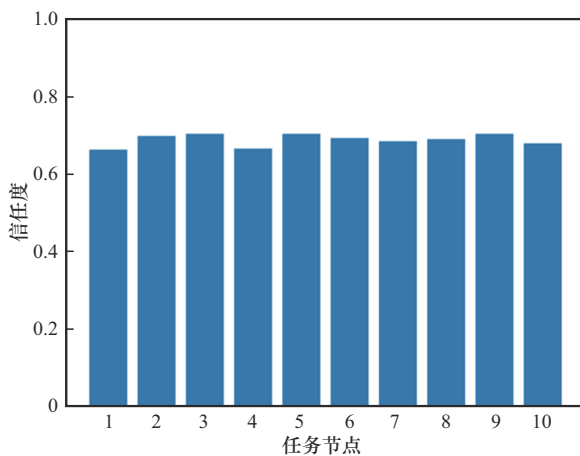


图 6 计算节点在某一时刻的信任度分布

Figure 6 Calculate the trust distribution of a node at a given point in time

之后, 记录了 5 个任务节点与计算节点在 30 次历史交互中的信任度变化对比, 如图 7 所示, 该计算节点

在30次交易中一直诚实地提供服务，信任度趋于上升状态，且每一时刻提取的信任度分布相对均匀。

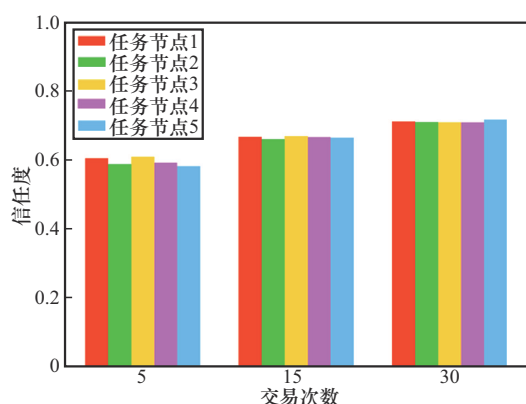


图7 各任务节点对同一节点在不同交易次数的信任度对比

Figure 7 Comparison of trust in the same node by task nodes at different trading counts

4.2.5 适应性函数的计算

使用直接信任度的变动程度设计适应性函数，动态调整直接信任度和间接信任度在总评估中的权重。直接信任度是任务节点基于历史交互对计算节点的直接观察。当直接信任度波动较大时，意味着计算节点新行为的出现改变了任务节点对其的直接信任程度，应当适时地调整信任度评估模型，赋予直接信任度更大的权重，以更好地反映任务节点的实际体验和期望。

4.2.6 平均耗时

本文评估了智能合约执行信任度评估的平均耗时。在一轮交易开始之前，假设有10个响应者，计算这10个响应者的信任度评估的平均耗时。实验结果如图8所示，信任数据上链的平均耗时约为77.49 ms，信任度计算的平均耗时约为37.92 ms，总体来看，耗时较少，表明所提的信任度评估模型实现了安全性和性能之间的平衡。

4.3 对比实验

现有的可信算力交易方案有些采用了区块链技术，通过智能合约自动执行交易和结算，确保交易的透明和不易篡改。但是此类方案缺少对交易参与节点的可信度评估，可能会增加交易风险。本文方案引入了信任度评估机制，可以有效评估节点信任度。与使用信任度评估机制的可信算力交易方案相比，本文方案更加注重交易方选择的公平性和节点反馈可靠性的度量。

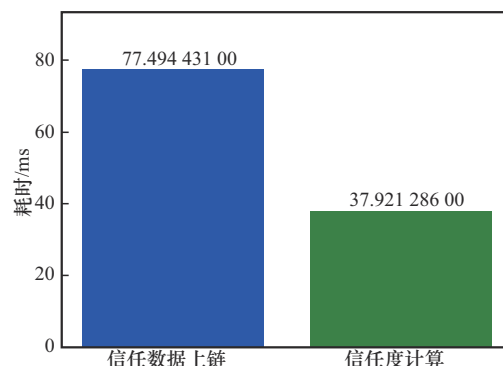


图8 智能合约执行信任度评估平均耗时

Figure 8 Smart contract execution trust assessment takes an average time

为了解本文方案的信任度评估能力，将本文方案与PeerTrust方案^[1]进行了对比实验。实验时，随机选取一个计算节点，查看其信任度随交易次数的变化。信任度评估对比实验结果如图9所示。当交易次数达到30次时，调整该节点的状态为恶意状态，提供恶意服务，从图9可以看出，本文方案对恶意节点的信任度明显下降。任务节点根据信任度的显著波动可以识别出计算节点状态的变化，从而区分出恶意节点和诚实节点；而PeerTrust方案是借助同行节点的信任度及节点相似度来衡量节点信任度的，在节点由诚实转为恶意的情况下，虽然信任度产生波动，但是短时间内仍然无法有效区分出恶意节点和诚实节点。综上所述，本文方案的信任度评估模型能够客观、全面地评估节点的可信度，识别恶意节点，同时能够有效评估节点反馈的可靠性。

5 结束语

针对算力网络环境下算力资源的泛在特性导致的交易参与方可信度不高问题，本文提出了一种基于信任度评估的分布式算力交易方案。该方案通过评估计算节点的信任度，为任务节点选择交易方提供依据，同时，设计了一种信任度评估模型，结合了基于反馈的直接信任和基于推荐的间接信任评估总信任度；此外，采用基于波动率的适应性函数动态调整直接和间接信任的权重，以解决信任度评估过程中的恶意评分和恶意服务所引起的信任度计算准确性低的问题；最后，结合区块链技术，将信任信息和交易记录存储到区块链中，以提高算力交易过程的透明性和不易篡

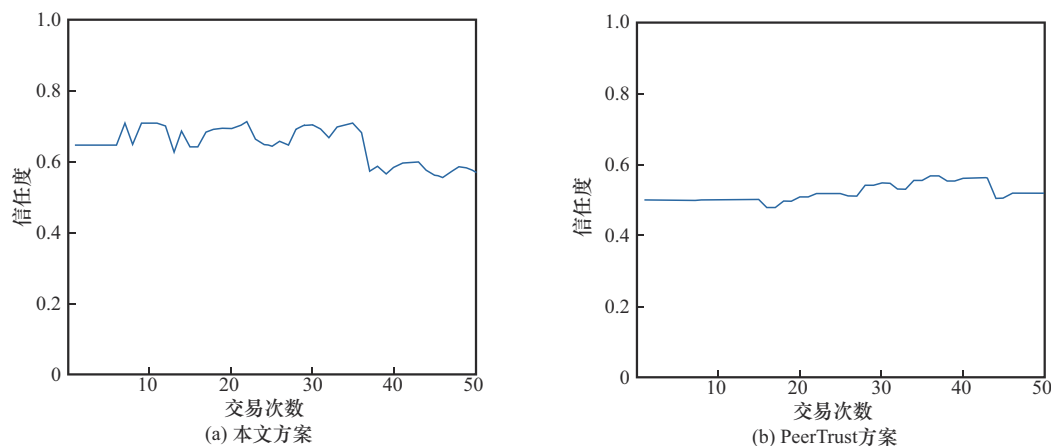


图9 信任度评估对比

Figure 9 Comparison of trust assessment

改性。未来,将进一步优化该方案的隐私保护能力,提升算力交易的隐私性和安全性。

参考文献:

- [1] LUO Q Y, HU S H, LI C L, et al. Resource scheduling in edge computing: a survey[J]. IEEE Communications Surveys & Tutorials, 2021, 23(4): 2131-2165.
- [2] 贾庆民, 丁瑞, 刘辉, 等. 算力网络研究进展综述[J]. 网络与信息安全学报, 2021, 7(5): 1-12.
JIA Q M, DING R, LIU H, et al. Survey on research progress for compute first networking[J]. Chinese Journal of Network and Information Security, 2021, 7(5): 1-12.
- [3] LIU Y J, WANG J, YAN Z, et al. A survey on blockchain-based trust management for internet of things[J]. IEEE Internet of Things Journal, 2023, 10(7): 5898-5922.
- [4] 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 S Q, HUO R, HUANG T, et al. A review of blockchain technology: principles, progress and applications[J]. Journal on Communications, 2020, 41(1): 134-151.
- [5] ANDONI M, ROBU V, FLYNN D, et al. Blockchain technology in the energy sector: a systematic review of challenges and opportunities[J]. Renewable and Sustainable Energy Reviews, 2019, 100: 143-174.
- [6] REN X, QIU C, WANG X, et al. AI-bazaar: A cloud-edge computing power trading framework for ubiquitous AI services[J]. IEEE Transactions on Cloud Computing, 2022, 11(3): 2337-2348.
- [7] 吕航, 李佳聪, 雷波, 等. 基于智能合约与区块链的算力交易机制[J]. 中兴通讯技术, 2022, 28(4): 52-57.
LYU H, LI J C, LEI B, et al. Computing power trading mechanism based on smart contract and blockchain[J]. ZTE Technology Journal, 2022, 28(4): 52-57.
- [8] WANG D, DU X, ZHANG H, et al. Blockchain enabled credible computing resource sharing: a multi-leader multi-follower stackelberg game approach[J]. IEEE Transactions on Vehicular Technology, 2024, 73(9): 13839-13852.
- [9] LIN X, WU J, MUMTAZ S, et al. Blockchain-based on-demand computing resource trading in IoV-assisted smart city[J]. IEEE Transactions on Emerging Topics in Computing, 2020, 9(3): 1373-1385.
- [10] 雷波, 陈运清, 王旭亮, 等. 边缘计算与算力网络——5G+AI时代的新型算力平台与网络连接[M]. 北京: 电子工业出版社, 2020.
LEI B, CHEN Y Q, WANG X L, et al. Edge computing and arithmetic networking: a new arithmetic platform and network connectivity in the 5G+AI era[M]. Beijing: Publishing House of Electronics Industry, 2020.
- [11] ZHANG M W, YANG M X, SHEN G, et al. A verifiable and privacy-preserving cloud mining pool selection scheme in blockchain of things[J]. Information Sciences, 2023, 623: 293-310.
- [12] KWANTWI T, SUN G L, KUADEY N A E, et al. Blockchain-based computing resource trading in autonomous multi-access edge network slicing: a dueling double deep Q-learning approach[J]. IEEE Transactions on Network and Service Management, 2023, 20(3): 2912-2928.
- [13] 王贺立, 闫巧. 基于交易记录特征的自私挖矿检测方案[J]. 网络与信息安全学报, 2023, 9(2): 104-114.
WANG H L, YAN Q. A selfish mining detection scheme based on transaction record features[J]. Chinese Journal of Network and Information Security, 2023, 9(2): 104-114.
- [14] WU X H, YU F J, WANG J, et al. BPF-payment: fair payment for cloud computing with privacy based on blockchain and homomorphic encryption[J]. Peer-to-Peer Networking and Applications, 2023, 16(5): 2649-2666.
- [15] LI Z N, YANG Z Y, XIE S L, et al. Credit-based payments for fast computing resource trading in edge-assisted internet of things[J]. IEEE Internet of Things Journal, 2019, 6(4): 6606-6617.
- [16] FAN S Z, ZHANG H B, ZENG Y C, et al. Hybrid blockchain-based resource trading system for federated learning in edge computing[J]. IEEE Internet of Things Journal, 2020, 8(4): 2252-2264.
- [17] 余佳仁, 田有亮, 林晖. 基于信誉管理模型的矿工类型鉴别机制设计[J]. 网络与信息安全学报, 2022, 8(1): 128-138.
YU J R, TIAN Y L, LIN H. Design of miner type identification mechanism based on reputation management model[J]. Chinese Journal of Network and Information Security, 2022, 8(1): 128-138.
- [18] CHENG H J, HU Q H, ZHANG X Q, et al. Trusted resource allocation based on smart contracts for blockchain-enabled internet of things[J]. IEEE Internet of Things Journal, 2021, 9(11): 7904-7915.

- [19] 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.
- WEN Y, LU J J, LU H, et al. Research on trust assessment and guarantee scheme for arithmetic network integrating blockchain[J]. Journal of Nanjing University of Posts and Telecommunications (Natural Science Edition), 2021, 41(4): 99-106.
- [20] LU Z J, QU G, LIU Z L. A survey on recent advances in vehicular network security, trust, and privacy[J]. IEEE Transactions on Intelligent Transportation Systems, 2018, 20(2): 760-776.
- [21] SAIED Y B, OLIVEREAU A, ZEGHLACHE D, et al. Trust management system design for the internet of things: a context-aware and multi-service approach[J]. Computers & Security, 2013, 39: 351-365.
- [22] AWAN K A, DIN I U, ALMOGREN A, et al. NeuroTrust: artificial-neural-network-based intelligent trust management mechanism for large-scale internet of medical things[J]. IEEE Internet of Things Journal, 2020, 8(21): 15672-15682.
- [23] XIONG L, LIU L. PeerTrust: supporting reputation-based trust for peer-to-peer electronic communities[J]. IEEE transactions on Knowledge and Data Engineering, 2004, 16(7): 843-857.
- [24] BHATTACHARJEE S, MADHAVARAPU V P K, SILVESTRI S, et al. Attack context embedded data driven trust diagnostics in smart metering infrastructure[J]. ACM Transactions on Privacy and Security(TOPS), 2021, 24(2): 1-36.
- [25] LE V T, EL IOINI N, BARZEGAR H R, et al. Trust management for service migration in multi-access edge computing environments[J]. Computer Communications, 2022, 194: 167-179.
- [26] REN J Y, QIN T F. A novel multidimensional trust evaluation and fusion mechanism in fog-based internet of things[J]. Computer Networks, 2022, 217: 109354.
- [27] MOUSTAFA A, ZHANG M J, BAI Q. Trustworthy stigmergic service composition and adaptation in decentralized environments[J]. IEEE Transactions on services computing, 2014, 9(2): 317-329.
- [28] 杨明, 胡学先, 张启慧, 等. 基于信誉评估机制和区块链的移动网络联邦学习方案[J]. 网络与信息安全学报, 2021, 7(6): 99-112.
- YANG M, HU X X, ZHANG Q H, et al. A mobile network federalism scheme based on reputation assessment mechanism and blockchain[J]. Chinese Journal of Network and Information Security, 2021, 7(6): 99-112.
- [29] HUANG C Y, WANG Z Y, CHEN H X, et al. REPChain: a reputation-based secure, fast, and high incentive blockchain system via sharding[J]. IEEE Internet of Things Journal, 2020, 8(6): 4291-4304.
- [30] AL-KHAFAJIY M, BAKER T, ASIM M, et al. COMMITMENT: a fog computing trust management approach[J]. Journal of Parallel and Distributed Computing, 2020, 137: 1-16.
- [31] KOUICEM D E, IMINE Y, BOUABDALLAH A, et al. Decentralized blockchain-based trust management protocol for the internet of things[J]. IEEE Transactions on Dependable and Secure Computing, 2020, 19(2): 1292-1306.
- [32] LIU H, HAN D Z, LI D. Behavior analysis and blockchain based trust management in vanets[J]. Journal of Parallel and Distributed Computing, 2021, 151: 61-69.
- [33] KUDVA S, BADSHA S, SENGUPTA S, et al. A scalable blockchain based trust management in VANET routing protocol[J]. Jour-

nal of Parallel and Distributed Computing, 2021, 152: 144-156.

- [34] LIU Y, ZHANG C, YAN Y, et al. A semi-centralized trust management model based on blockchain for data exchange in IoT system[J]. IEEE Transactions on Services Computing, 2022, 16(2): 858-871.
- [35] DU G X, CAO Y J, LI J, et al. A blockchain-based trust-value management approach for secure information sharing in internet of vehicles[J]. IEEE Internet of Things Journal, 2023, 11(1): 333-344.

[作者简介]



王英晓春(1998-), 女, 山东青岛人, 齐鲁工业大学(山东省科学院)硕士生, 主要研究方向为数据安全、区块链应用。



王连海(1969-), 男, 山东潍坊人, 齐鲁工业大学(山东省科学院)/山东省计算中心(国家超级计算济南中心)研究员, 主要研究方向为数据安全、区块链、计算机取证。



徐淑奖(1979-), 男, 山东临沂人, 齐鲁工业大学(山东省科学院)/山东省计算中心(国家超级计算济南中心)研究员, 主要研究方向为数据安全、区块链。



张淑慧(1981-), 女, 山东济宁人, 齐鲁工业大学(山东省科学院)/山东省计算中心(国家超级计算济南中心)研究员, 主要研究方向为数据安全、区块链、计算机取证。



刘天瑞(1995-), 男, 山东济南人, 齐鲁工业大学(山东省科学院)硕士生, 主要研究方向为区块链技术、联邦学习。