基于区块链的算网可信交易激励机制研究

张桂玉[1]，刘博文[1]，梁晓晨[1]，张笑颜[1]，吕城锦[1]，于思佳[1]，李硕[2]
（1.中讯邮电咨询设计院有限公司，北京 100089；2.北京邮电大学网络与交换国家重点实验室，北京 100876）

摘　要：随着基于智能合约的云网资源交易技术的发展，算力交易向多方规模的形式发展，严重影响算网资源的高效可信交易。针对算力网络资源多方参与场景下的可信交易与高效资源激励需求，设计基于区块链的算网资源可信身份认证与资源交易激励机制。该机制采用基于算网用户身份信息可靠度的分布式认证策略，通过公证机构授权构建可信交易委托证书，实现资源交易任务可信进行。讨论基于契约理论的交易激励机制在算网资源可信交易与高效性服务上的应用，并与线性激励、信托激励模型进行机制对比，对算网参与方的资源效用收益与社会福利进行比较，进行多方最优效用收益激励验证，衡量本机制的激励效率。证明资源交易激励机制在交易验证场景的有效性，有效保证算网资源在多服务方接入的可信交易与高效激励。实验结果显示，该交易机制能够保障多方算网用户交易的可信性、可验证性与稳定性。所提机制在资源交易效率与社会福利收益方面均优于传统交易激励机制。

关键词：算力网络；区块链；分布式身份认证；资源交易激励
中图分类号：TP393
文献标志码：A
DOI：10.11959/j.issn.2096−109x.2024062

Research on the incentive mechanism of trusted transactions based on blockchain

ZHANG Guiyu[1], LIU Bowen[1], LIANG Xiaochen[1], ZHANG Xiaoyan[1],
LYU Chengjin[1], YU Sijia[1], LI Shuo[2]
1. China Information Technology Designing Consulting Institute Co., Ltd.，Beijing 100089, China
2. Stale Key Laboratory of Networking and Switching Technology，
Beijing University of Posts and Telecommunications, Beijing 100876, China

Abstract: With the development of cloud-network resource transaction technology based on smart contracts, computing power transactions have reached a multi-party scale, seriously affecting the efficiency and credibility of computing network resource transactions. To meet the requirements of trusted transactions and efficient resource incentives in the scenario of multi-party participation in computing network resources, a blockchain-based trusted identity authentication and resource transaction incentive mechanism for computing network resources was designed. The mechanism adopted a distributed authentication strategy based on the reliability of user identity information of

收稿日期：2024−02−29；**修回日期：**2024−07−28
通信作者：李硕，muzishige@bupt.edu.cn

引用格式：张桂玉, 刘博文, 梁晓晨, 等. 基于区块链的算网可信交易激励机制研究[J]. 网络与信息安全学报, 2024, 10(4): 175-186.
Citation Format: ZHANG G Y, LIU B W, LIANG X C, et al. Research on the incentive mechanism of trusted transactions based on blockchain[J]. Chinese Journal of Network and Information Security, 2024, 10(4): 175-186.

the computing network and constructed a trusted transaction entrustment certificate through the authorization of an impartial agency, realizing the trusted implementation of resource transaction tasks. In addition, the application of the transaction incentive mechanism based on contract theory in the trusted transaction and efficient service of computing network resources was discussed. The mechanism was compared with linear incentive and trust incentive models, and the resource utility income and social welfare of the computing network participants were compared. The multi-party optimal utility benefit incentive was verified to measure the incentive efficiency of the mechanism. It proved the effectiveness of the resource transaction incentive mechanism in the transaction verification scenario and effectively ensured the trusted transaction and efficient incentive of computing network resources accessed by multiple service parties. Experimental results show that the proposed transaction mechanism could ensure the credibility, verifiability, and stability of multi-party computing network user transactions. The proposed mechanism is superior to the traditional transaction incentive mechanism in terms of resource transaction efficiency and social welfare benefits.

Keywords: computing power network, blockchain, distributed identity authentication, resource transaction incentive

0　引 言

随着信息通信技术的不断迭代，传统的云网计算与网络技术逐渐融合，逐渐拓展成为“计算+网络+协同”的算力网络技术。在算力网络集中式的资源管理模式下，算网中心可以通过有效的资源分配和调度来实现更好的资源性能和扩展性[1]。同时去中心化资源节点分布方式减少了对单一中心实体的依赖，提高了系统的稳定性。然而，集中式交易管理产生的海量信息增加了信息处理的负担，并且在现有的计算网络资源处理中，常见的资源交易场景是区块链模型下单个代理与多方需求之间的收入匹配问题，而考虑区块链在资源信息安全问题并不全面，因此如何提高信息处理效率并保证用户信息安全可信就显得尤为重要[2]。

然而，上述集中式的算网平台还存在以下问题，制约算网可信交易和高效交易的实现。①在现有的计算网络资源处理中，常见的资源交易场景是区块链模型下单个代理与多方需求之间的收入匹配问题，而考虑区块链在资源信息安全问题并不全面；②由于算网用户需求和服务场景的多样化，精确匹配计算网络资源并激励供应商贡献其高质量的计算能力资源的方案尚不成熟，不利于资源的高效交易。

学术界针对算网平台中的可信高效交易提出了一些方案，但方案考虑不全面，无法完全支撑可信高效交易，仍处于研究的初期探索阶段。由于算力服务网络中资源交易信息的多维异构，保障算网资源交易的可信性显得尤为重要。在可信交易的趋势下，将分布式认证技术融入算网资源交易已成为实现算网可信交易的有效手段，这是当前算网可信交易的主要方向之一。刘乃安等[3]关注区块链身份共识证明中的积极性问题。提出了一种面向区块链验证节点的声誉证明共识机制，该机制通过交互指标表示节点在区块网络中的贡献度，评估可靠度，提升声誉权重。李莉等[4]探讨了如何利用区块链技术构建资源共享平台，该平台确保了数据的安全存储性、健壮性和可信性，降低了数据资源中心化的程度，同时保障了用户的个人财产利益和避免了数据泄露等问题。徐杨杨等[5]针对云制造平台中虚拟化的制造资源在交易过程中难以保证数据真实性和安全性，提出了一种基于区块链的云制造资源分配方法。他们首先设计了基于区块链的去中心化的云制造交易平台框架，并研究制造资源与需求匹配的机制；然后，利用智能合约设计了面向云制造的制造资源校验合约和制造资源交易合约。

因此，为实现算力网络资源流通的可信交易与高效交易，针对算网资源交易过程中的可信交易问题，本文将区块链技术与身份认证技术相结合，研究设计了基于证书的身份认证的区块链交易策略，实现可信算网交易。为激励资源供应方贡献其算网资源到服务资源市场，本文构建了资源供应方与算力平台的动态博弈激励模型，实现了动态资源激励供应与高效激励。

1　相关理论基础

本文基于区块链技术不可更改的优势以及身

份认证技术的信息认证特点，为算网资源交易设计了可信资源交易流程，进一步保证了资源交易的安全性。同时基于博弈理论，构建了资源供应方与算网平台的资源博弈模型。

1.1　区块链关键理论

区块链是由节点参与的分布式数据库系统，它的特点是难以更改、不可伪造，也可以将其理解为账簿系统。通过这些信息，可以找到每一个地址在历史上任何一点拥有的价值。区块链核心技术主要以密码学、共识机制与分布式存储技术为基础，并在此基础上逐渐拓展应用[6]。

1.2　身份认证技术

身份认证是证实实体对象的数字身份与物理身份是否一致的过程。身份认证技术能够有效防止信息资源被非授权使用，保障信息资源的安全[7]。

1）基于证书的身份认证：基于证书认证是基于用户的数字证书。基于证书的认证机制借助于公钥基础设施体系，由 CA（certificate authority）为设备的公钥进行签名, 使系统内的其他设备都可以使用 CA 的公钥对该证书进行合法性验证, 验证成功则认可该证书中提供的设备公钥。

2）基于密码的身份认证：基于密码的身份验证依赖于用户名和密码或 PIN。不过基于密码的身份验证是攻击者最容易滥用的身份验证类型。人们经常重复使用密码并使用字典单词和公开的个人信息创建可猜测的密码。

3）基于身份的身份认证：基于身份的认证机制是利用身份标识密码技术，核心是使用用户和设备具有唯一性和抗否认性的身份信息（例如用户的邮件地址、身份证号、电话号码等）计算出公钥，而不需要第三方机构保障公钥的真实性, 从而降低了系统的证书管理成本和对中心化机构的依赖。

综合比较 3 种常见的身份认证方式，基于证书的身份认证机制具有的强身份认证、安全性高、可靠性强、互操作性好和可撤销性的优势，确保在身份认证过程中的数据传输的保密性和完整性。基于证书的身份认证机制在多方面展现出的安全优势使它成为许多安全敏感应用和系统中首选的身份认证方法。

1.3　博弈竞争

博弈竞争是指在竞争环境中的参与者之间相互作用并做出决策的过程。在博弈竞争中，每个参与者追求自己的利益，并且他们的决策会相互影响并产生结果。

博弈论是研究博弈竞争的数学模型和策略的学科。它研究参与者之间的决策行为、策略选择、收益和结果，并通过分析和建模来推导最优决策或稳定解。

在博弈竞争中，常见的博弈模型包括零和博弈、非零和博弈和合作博弈等。

2　基于服务认可度的可信交易策略

在算网资源交易过程中，为实现可信交易，进一步保障资源信息安全性，本文方案采用身份认证技术与联盟链可信技术设计了可信身份管理与可信交易流程方案[7-8]。在可信身份管理层面，本文交易方案需要对算力资源供应方、需求方进行身份注册与身份认证流程，进一步保证资源需求的可靠性。在可信交易流程中，基于联盟链多方节点认证的资源交易电子合同将会进一步保证交易的可靠性。

2.1　可信身份管理机制

可信身份管理主要通过基于证书的身份认证技术实现，基于原有的 X.509 证书，设计区块链身份证书，实现可信身份注册与可信身份认证过程。

为实现身份管理流程在算网平台上的服务交互性、可访问性与用户友好性。用户可采用需求表单输入的方式提交资源需求。通过设计直观易用的用户界面与图标和标识，身份注册过程对资源指标信息、算力用户信息进行收集。身份认证过程对注册信息进行验证，通过联盟链上信息与数字证书进行对比，确定用户信息可靠性。针对用户友好性，算网平台提供多种身份验证方式，包括密码、生物识别、硬件密钥等，让用户可以选择适合自己的认证方式，提高系统的安全性和可接受性。针对服务质量信息，收集用户服务信息反馈，并及时对用户的意见和建议进行响应和改进。通过持续的用户体验改进，不断提升系统的用户友好性和可访问性，满足用户需求。

2.1.1　身份注册

传统的公钥基础设施验证数字证书的完整性是通过验证数字签名来实现的，以确保数字证书中的身份和公钥是可信的。传统的X.509数字证书如图1所示。X.509数字证书采用公钥与私钥的秘钥对结构。公钥负责对信息进行加密，而对应的私钥负责解密信息，从而保证发送者的身份信息与发送信息的安全性[8-9]。X.509数字证书标准字段主体结构包括签名算法识别符、有效期、主体公钥信息与签名信息，X.509数字证书的双方信任结构、可扩展性等特点在保障网络交互信息领域展现出相应的优势。因此本文在X.509的基础上，设计了区块链证书，该证书如图2所示。

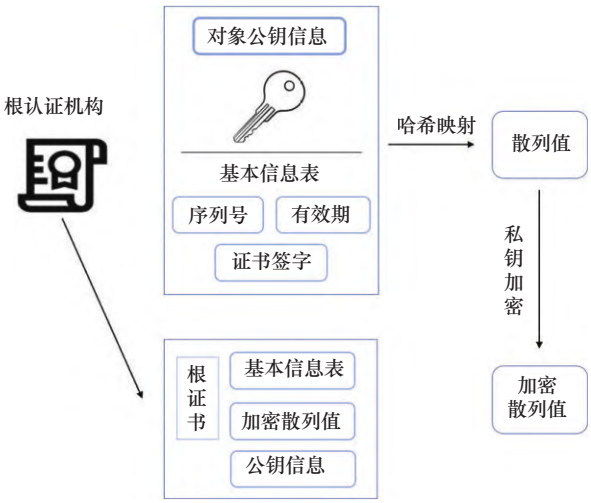

图1　X.509证书

Figure1　X. 509 certificate

用户在首次使用该系统时需要注册身份信息，进入系统后就无须再次注册。用户向CA发送注册信息，CA验证合法性后生成用户公钥和私钥。随后，CA在区块链证书中包括用户身份和公钥，并对这些信息进行哈希运算，以生成证书的哈希值，然后，将证书和哈希值存储在区块链上。最后，CA向用户返回认证成功的信息，用户成功注册。若证书不合法，则注册失败。

2.1.2　身份认证过程

基于证书的身份认证过程包括以下步骤。

1）注册：身份验证的实体首先向认证机构注册，并提供一些基本信息，如名称、电子邮件、地址等。

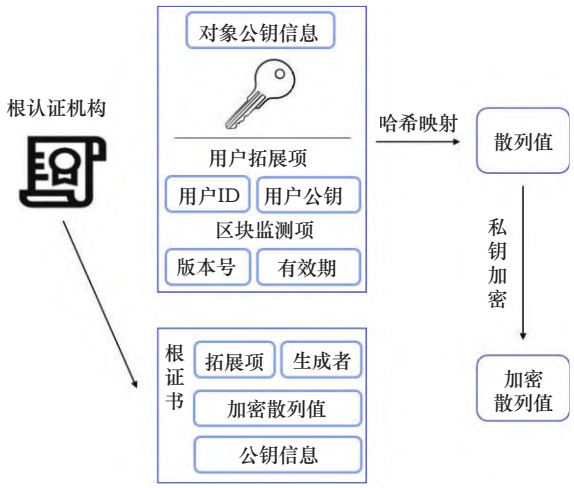

图2　区块链证书

Figure 2　Blockchain certificate

2）生成密钥对：在注册之后，实体会生成一对密钥，包括公钥和私钥。私钥必须保持私密，而公钥可以在需要时公开。

3）证书请求：实体需要向认证机构请求生成一个数字证书。证书由认证机构使用其私钥对实体的公钥进行数字签名生成。证书除了实体的公钥，还包含一些其他信息，如实体的名称、电子邮件、地址等。

4）证书签名：认证机构收到证书请求后，会验证该请求，并使用其私钥对实体的公钥进行数字签名。签名是通过对证书中的信息进行哈希处理，然后使用认证机构的私钥进行加密生成的。

5）证书颁发：认证机构将签名后的证书返回给实体。这个证书就是实体的数字身份证明，在后续的通信中将用于身份验证。

6）身份验证：当实体需要进行身份验证时，它会发送证书给对方。对方收到证书后，会使用认证机构的公钥解密证书中的签名来验证证书的真实性。验证包括验证签名是否有效、证书是否在有效期内、证书是否被撤销等。

7）客户端认证和服务器认证：基于证书的身份认证可以用于客户端认证和服务器认证。对于客户端认证，客户端向服务器发送证书以证明其身份；对于服务器认证，服务器向客户端发送证书以证明自己的身份。

与传统基于 PKI/CA 的身份认证过程相比，本文的身份认证在交易过程中，可以采用数字证书作为身份标识，并使用私钥对交易信息进行签名，以实现身份认证和交易的安全性，并进一步降低了传统 PKI/CA 身份认证重复构建数字证书的烦琐性。数字证书包含了用户的公钥以及相关身份信息，并由可信的证书颁发机构进行签发和验证。用户可以使用其私钥对交易信息进行签名，证明其身份的合法性和交易的真实性。这种方式能够有效防止身份被伪造和信息被篡改，确保交易的安全可靠。

基于证书的身份认证过程依赖于 CA 机构的可信性和证书的完整性。它提供了一种可靠的身份验证机制，并确保通信的保密性和完整性。

2.2　可信交易流程设计

在完成可信身份管理与身份认证的基础上，基于身份认证与联盟链技术，本文设计了相应的可信交易流程，步骤如下。

1）交易平台对算力需求方进行身份认证。

2）交易平台接受算力资源需求标准制定调度策略。

3）执行调度策略得到推荐平台用户购买的算网资源商品组合购买方案。

4）交易平面制定电子合同，电子合同包括可供使用的资源、最终报价、服务保障等。电子合同的数据结构如图3所示。

图3　电子合同的数据结构

Figure 3　Date structure electronic contract

5）设算力需求方选择第 i 个组合购买方案、平台用户与供应方合同。

6）算力需求方与平台签约，电子合同上链，需求方同时向平台支付金额，金额为2）确定的总价，金额由平台暂存，待交易完成后转入算力提供者账户。

7）算网资源商品服务完成后，平台对算力提供者进行评分更新。评分由客观评分和主观评分组成，评分更新后上链。

8）平台将金额转入算力提供者账户。

为保障算力提供方的服务质量，设置了提供方服务质量评分机制。如果服务质量评分低于一定阈值，平台会扣除提供方获得的金额，扣除部分返还给用户，平台通过评分机制可以约束算力提供方的行为。

本交易流程与传统联盟链可信交易相比，进一步扩展了上链信息的完整度，将算力需求方的资源签约合同与服务金额进行平台暂存，确保算力交易的可靠性。另外，本交易流程设计引入了传统区块链交易的交易评价机制，对资源服务完成后的评分信息进行更新上链，进一步保障算力用户的服务质量。本交易区块链的设计弥补了传统区块链交易信息的残缺部分，完整地考虑了算网交易完成前后的交易信息，保障算力供应方与用户双方的服务权益。

3　基于算力资源动态博弈定价的激励机制

为激励资源供应方贡献出其合适的算网资源，本激励机制需考虑算网资源的多重属性，构建合适的资源匹配奖励机制[9-10]。本激励机制在综合考虑供应方资源收益与算力平台综合收益的基础上，对算网资源进行度量动态定价建模，考虑资源需求方需求指标与资源市场动态浮动因素，构建动态定价激励模型。最终的资源激励模型，考虑供应方与算力平台的最优收益可简化为最优收益优化问题。

3.1　多维异构资源的度量模型

算力网络服务中的参与方包括传统云服务基础设施、边缘基础设施、终端设备等，实现对多参与方提供的异构算网资源的统一度量建模是算网服务的基础，算网资源主要包括计算资源、存储资源和网络资源[13-14]。具体算网资源的性能影响指标数量也存有差异，定义计算资源、网络资源、存储资源指标集合 $N_{\text{inf}} \in \left\{N_{\text{inf}}^{\text{cpt}}, N_{\text{inf}}^{\text{sto}}, N_{\text{inf}}^{\text{net}}\right\}$，其中，$N_{\text{inf}}^{\text{cpt}}$ 为计算资源性能指标数量，$N_{\text{inf}}^{\text{sto}}$ 为存储

资源性能指标数量，$N_{\text{inf}}^{\text{net}}$ 为网络资源性能指标数量。

（1）计算资源建模

综合主频、睿频、核数、线程数、缓存、内存容量、显存、内存带宽等测量指标对计算资源综合性能（质量）进行衡量。

计算资源的性能参数向量可定义为：

$$\boldsymbol{v}^{\text{cpt}}=\left(v_1^{\text{cpt}},v_2^{\text{cpt}},\cdots,v_{N_{\text{inf}}^{\text{cpt}}}^{\text{cpt}}\right) \tag{1}$$

其中，v_i^{cpt} 表示计算资源的第 i 个性能参数，$N_{\text{inf}}^{\text{cpt}}$ 表示计算资源性能参数的个数。定义 q^{cpt} 表示衡量计算资源的综合评价指标，根据计算资源的性能参数向量，通过加权平均方式得出该规格计算资源的计算能力综合评价指标：

$$\begin{aligned}q^{\text{cpt}}\left(\boldsymbol{v}^{\text{cpt}}\right)=&\left(\alpha_1^{\text{cpt}},\cdots,\alpha_{N_{\text{inf}}^{\text{cpt}}}^{\text{cpt}}\right)\cdot\\&\left(f_1^{\text{cpt}}\left(v_1^{\text{cpt}}\right),\cdots,f_{N_{\text{inf}}^{\text{cpt}}}^{\text{cpt}}\left(v_{N_{\text{inf}}^{\text{cpt}}}^{\text{cpt}}\right)\right)^{\text{T}}\end{aligned} \tag{2}$$

其中，$\left(\alpha_1^{\text{cpt}},\alpha_2^{\text{cpt}},\cdots,\alpha_{N_{\text{inf}}^{\text{cpt}}}^{\text{cpt}}\right)$为计算资源性能参数对应的权重系数，且有 $\sum_1^{N_{\text{inf}}^{\text{cpt}}}\alpha_i^{\text{cpt}}=1,\forall i\in\left[1,N_{\text{inf}}^{\text{cpt}}\right]$，$\alpha_i^{\text{cpt}}\in[0,1]$。$f_i^{\text{cpt}},\forall i\in\left[1,N_{\text{inf}}^{\text{cpt}}\right]$将性能参数映射到计算能力综合评价指标的加权公式中。线性函数 f_i^{cpt} 衡量计算资源指标 v_i^{cpt} 的算力质量，v_i^{cpt} 指标越高 $f_i^{\text{cpt}}(v_i^{\text{cpt}})$ 算力质量越好。

（2）存储资源建模

存储资源的存储能力主要涉及存储容量、存储带宽和每秒读写操作数（input/output per second，IOPS）及响应时间等指标。

存储资源的参数向量可定义为：

$$\boldsymbol{v}^{\text{sto}}=\left(v_1^{\text{sto}},v_2^{\text{sto}},\cdots,v_{N_{\text{inf}}^{\text{sto}}}^{\text{sto}}\right) \tag{3}$$

其中，v_i^{sto} 表示存储资源的第 i 个参数，$N_{\text{inf}}^{\text{sto}}$ 表示存储资源参数的个数。定义 q^{sto} 表示衡量存储资源的综合评价指标，根据存储资源的性能参数向量，通过加权平均方式得出该规格资源的存储能力综合评价指标：

$$\begin{aligned}q^{\text{sto}}\left(v^{\text{sto}}\right)=&\left(\alpha_1^{\text{sto}},\cdots,\alpha_{N_{\text{inf}}^{\text{sto}}}^{\text{sto}}\right)\cdot\\&\left(f_1^{\text{sto}}\left(v_1^{\text{sto}}\right),\cdots,f_{N_{\text{inf}}^{\text{sto}}}^{\text{sto}}\left(v_{N_{\text{inf}}^{\text{sto}}}^{\text{sto}}\right)\right)^{\text{T}}\end{aligned} \tag{4}$$

其中，$\left(\alpha_1^{\text{sto}},\alpha_2^{\text{sto}},\cdots,\alpha_{N_{\text{inf}}^{\text{sto}}}^{\text{sto}}\right)$为存储资源性能参数对应的权重系数，且有 $\sum_1^{N_{\text{inf}}^{\text{sto}}}\alpha_i^{\text{sto}}=1,\forall i\in\left[1,\alpha_{N_{\text{inf}}^{\text{sto}}}^{\text{sto}}\right]$，$\alpha_i^{\text{sto}}\in[0,1]$。$f_i^{\text{sto}},\forall i\in\left[1,N_{\text{inf}}^{\text{sto}}\right]$将性能参数映射到存储能力综合评价指标的加权公式中。线性函数 f_i^{sto} 衡量计算资源指标 v_i^{sto} 的算力质量，v_i^{sto} 指标越高 $f_i^{\text{sto}}(v_i^{\text{sto}})$ 算力质量越好。

（3）网络资源建模

网络资源的网络质量主要是对节点对外交互过程中网络速率和网络的评估。通过加权平均方式得出该规格资源的网络能力综合评价指标。

网络资源的参数向量可定义为：

$$\boldsymbol{v}^{\text{net}}=\left(v_1^{\text{net}},v_2^{\text{net}},\cdots,v_{N_{\text{inf}}^{\text{net}}}^{\text{net}}\right) \tag{5}$$

其中，v_i^{net} 表示网络资源的第 i 个参数，$N_{\text{inf}}^{\text{net}}$ 表示网络资源参数的个数。定义 q^{net} 表示衡量存储资源的综合评价指标，根据网络资源的性能参数向量，通过加权平均方式得出该网络资源的网络质量综合评价指标：

$$\begin{aligned}q^{\text{net}}\left(v^{\text{net}}\right)=&\left(\alpha_1^{\text{net}},\cdots,\alpha_{N_{\text{inf}}^{\text{net}}}^{\text{net}}\right)\cdot\\&\left(f_1^{\text{net}}\left(v_1^{\text{net}}\right),\cdots,f_{N_{\text{inf}}^{\text{net}}}^{\text{net}}\left(v_{N_{\text{inf}}^{\text{net}}}^{\text{net}}\right)\right)^{\text{T}}\end{aligned} \tag{6}$$

其中，$\left(\alpha_1^{\text{net}},\alpha_2^{\text{net}},\cdots,\alpha_{N_{\text{inf}}^{\text{net}}}^{\text{net}}\right)$为网络资源性能参数对应的权重系数，且有 $\sum_1^{N_{\text{inf}}^{\text{net}}}\alpha_i^{\text{net}}=1,\ \forall i\in\left[1,N_{\text{inf}}^{\text{net}}\right]$，$\alpha_i^{\text{net}}\in[0,1]$。$f_i^{\text{net}},\forall i\in\left[1,N_{\text{inf}}^{\text{net}}\right]$将性能参数映射到网络质量综合评价指标的加权公式中。线性函数 f_i^{net} 衡量计算资源指标 v_i^{net} 的算力质量，v_i^{net} 指标越高 $f_i^{\text{net}}(v_i^{\text{net}})$ 算力质量越好。考虑算力网络节点的“算-网-存”3 个维度，节点的算网资源综合基本度量结果可表示为：

$$\begin{aligned}q_n^{\text{base}}=&\left(q^{\text{cpt}}\left(\boldsymbol{v}^{\text{cpt}}\right),q^{\text{sto}}\left(v^{\text{sto}}\right),q^{\text{net}}\left(v^{\text{net}}\right)\right)\cdot\\&\left(\gamma^{\text{cp}},\gamma^{\text{sto}},\gamma^{\text{net}}\right)^{\text{T}}\end{aligned} \tag{7}$$

其中，$\left(\gamma^{\text{cp}},\gamma^{\text{sto}},\gamma^{\text{net}}\right)$为计算资源性能参数对应的权重系数，且有 $\gamma^{\text{cp}}+\gamma^{\text{sto}}+\gamma^{\text{net}}=1,\gamma^{\text{cp}},\gamma^{\text{sto}},\gamma^{\text{net}}\in[0,1]$ 得到节点 n 的算力网络资源综合度量结果，q_n^{base} 可用于表征该节点的算力网络资源情况。

基于层次分析法确定计算、存储、网络资源的具体衡量指标之间的相对重要性，采用特征值分析法确定 α_i^{cpt}、α_i^{sto}、α_i^{net} 的取值范围。

表 1　权重取值范围

Table 1　The range of the weights

资源指标权重	α 取值范围
$\alpha_i^{\mathrm{cpt}},\ \forall i \in \left[1, \alpha_{N_{\mathrm{inf}}^{\mathrm{cpt}}}^{\mathrm{cpt}}\right]$	(0.05, 0.075)
$\alpha_i^{\mathrm{sto}},\ \forall i \in \left[1, \alpha_{N_{\mathrm{inf}}^{\mathrm{sto}}}^{\mathrm{sto}}\right]$	(0.25, 0.35)
$\alpha_i^{\mathrm{net}},\ \forall i \in \left[1, \alpha_{N_{\mathrm{inf}}^{\mathrm{net}}}^{\mathrm{net}}\right]$	(0.063, 0.092)

3.2　算网资源服务定价模型

算力交易平台上出售的算力供给方算力资源可以看作是一般市场中的商品，在算网交易资源定价前应当对算力资源从商品的角度出发并结合算力资源的具体特征建立商品模型。

用 m（$m \in M$）表示算力交易平台可提供的算网资源商品，商品总数为 $|M|$。算力资源商品 m（以下简称商品 m）的商品模型 c_m 建模如下：

$$c_m = \left\{ k_m \in K, a_m \in A, v_m^{\mathrm{para}} = \left(v_{m,1}^{\mathrm{para}}, v_{m,2}^{\mathrm{para}}, \cdots, v_{m,N_{k_m}^{\mathrm{para}}}^{\mathrm{para}} \right) \right\} \tag{8}$$

其中，k_m 是商品 m 所属的资源类型（如计算资源、存储资源、网络资源等，且可具体扩展），a_m 是商品 m 所属的地域（例如华南、华北等），v_m^{para} 是商品硬件参数向量（例如当商品属于计算资源时，参数向量表示的具体含义是主频、睿频、核数、线程数、缓存、内存容量、显存、网络带宽、内存带宽、GPU 吞吐量、GPU 显存容量等），N_{inf} 是商品 m 所属资源类型包含的参数数量。在商品定价函数中应当把基于商品模型中的参数映射得到的定价作为基本值。

资源商品定价函数 $q_m^{\mathrm{bas}}(c_m)$ 值为资源商品 m 的基础定价，其定义如下：

$$\begin{aligned} q_m^{\mathrm{bas}}(c_m) = &\left(\alpha_{k_m}^{\mathrm{area}}, \alpha_{1,k_m}^{\mathrm{para}}, \cdots, \alpha_{N_{inf},k_m}^{\mathrm{para}}, \right) \cdot \\ &\left(f_{k_m}^{\mathrm{area}}(a_m), f_{1,k_m}^{\mathrm{para}}\left(v_{m,1}^{\mathrm{para}}\right), \cdots, f_{N_{\mathrm{inf}},k_m}^{\mathrm{para}}\left(v_{m,N_{\mathrm{inf}}}^{\mathrm{para}}\right) \right)^{\mathrm{T}} \end{aligned} \tag{9}$$

其中，$q_m^{\mathrm{bas}}(c_m)$ 代表的算力商品基础定价仅与商品 m 本身模型 c_m 有关。$\alpha_{k_m}^{\mathrm{area}}$ 是商品 m 供给地域对应的价格模型系数，$\left(\alpha_{1,k_m}^{\mathrm{para}}, \alpha_{2,k_m}^{\mathrm{para}}, \cdots, \alpha_{N_{\mathrm{inf}},k_m}^{\mathrm{para}}\right)$ 为商品 m 的 N_{inf} 个硬件参数对应的价格模型系数。$f_{k_m}^{\mathrm{area}}$ 为衡量资源商品 m 所在地域的定价影响函数，考虑资源传输距离、地域定价策略等因素，算网资源商品 m 的服务距离越远，$f_{k_m}^{\mathrm{area}}$ 对基本定价的影响越强。$f_{i,k_m}^{\mathrm{para}} \in \left\{ f_i^{\mathrm{cpt}}, f_i^{\mathrm{sto}}, f_i^{\mathrm{net}} \right\}$ 将资源参数映射到价格计算的加权公式中，该系列函数也仅与商品 m 所属的商品类型 k_m 有关。

除基础定价以外，整个市场对于商品供需现状，其供需关系可动态影响，评分映射关系反映了商品综合评分对资源定价的影响能力，而供应商品最近时段内的交易数量，反映了市场对于供应商品的资源需求量（或供应商品的市场需求热度）。定价模型如图 4 所示。

基于以上分析供应商 j 商品 m 的定价 $p_{m,j}^{\mathrm{set}}$ 定义如下：

$$p_m^{\mathrm{set}} = q_m^{\mathrm{bas}}(c_m) \cdot \left(1 + f_u\left(\pi_m^T\right) + f_e\left(e_m^{\mathrm{tol}}\right)\right) \tag{10}$$

其中，$f_u\left(\pi_m^T\right)$ 为资源供需关系调整参量，$f_e\left(e_m^{\mathrm{tol}}\right)$ 为资源质量评价调整参量，$f_u\left(\pi_m^T\right), f_e\left(e_m^{\mathrm{tol}}\right)$ 作为动态因素影响算网资源定价。

3.3　算网资源动态激励

算力需求方的业务需求和算力市场的供求关系复杂多变，算力供应方的资源定价也不应该是一成不变的，为了使资源定价能准确地反映市场情况，也为了需求方和供应方都能得到较公平的回报，激励机制还需考虑定价更新策略，定价更新策略包括周期性更新和触发式更新两种[12-13]。平台确定和更新定价的流程如下。

1）算力供应方注册服务后，平台根据其服务能力和供应方通过契约理论规定初始价格，该价格由供应方资源质量决定，平台方并不会参与初始价格的变更博弈，因此在供应方注册加入后，初始价格仅由资源质量决定，平台会收集供应方的初始资源信息，考量该资源质量等级与价格的匹配程度。

2）算力供应方加入平台一段时间后，平台会设定后台信息刷新周期，通过调研得到各平台服务刷新时间，此周期设定以一周为单位，并保留此供应方两周内的节点热度、服务质量评分与节点位置等信息，作为质量评分参考。

3）在周期 T 内收集得到的质量信息，如节点热度、服务质量评分、请求位置与用户评价等信息，会以满意度的形式反馈给算力平台，平台

根据该供应方信息满意度与其进行周期博弈以更新资源价格。基于周期资源质量信息评定机制，算力平台能够得到供应方全面可靠的资源信息，用于动态调整平台与供应方之间博弈价格。

4）平台除了周期性更新定价，还需考虑实际市场的情况，比如某段时间用户的数量变化较大或算力节点的数量变化较大而导致供求关系改变。

5）当市场资源某种类型所需资源的供应关系出现大幅度变化时，算力平台为给予算力供应方的一定自由度，当算力供应方有意愿修改定价时，算力供应方可以向平台发起定价修改请求，这是由供应方发起的触发式价格更新。由3）和4）可知，该触发式定价更新是平台和供应方的双向更新。

从图5价格更新结构可以看出，无论是周期性价格更新还是触发式价格更新，都会重复执行该价格确定方案。

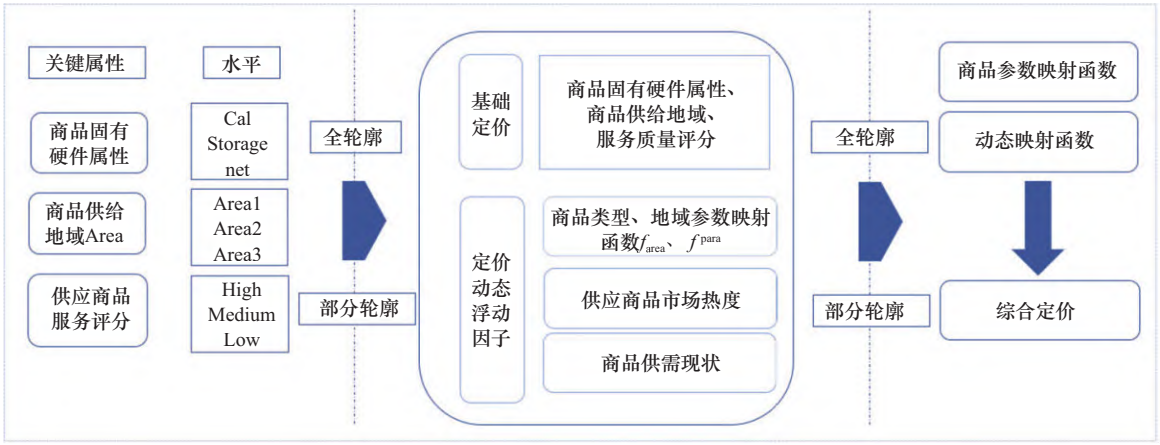

图4　算网资源商品定价模型

Figure 4　Commodity pricing model for computing network resources

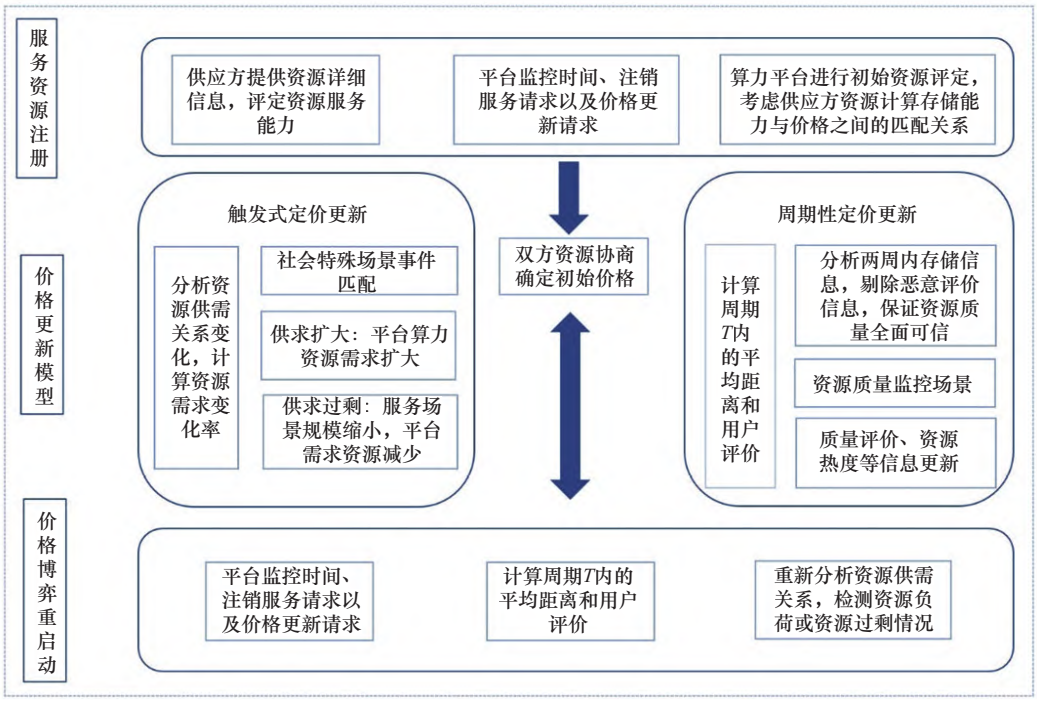

图5　价格更新结构

Figure 5　Scoring block charts

根据平台与供应方的协商流程，可划分为注册加入场景、普通周期更新场景与触发式协商场景。

3.4　算力供应方最优商品收益

对于算力交易过程，算力平台会根据供应商的资源商品模型和资源需求，接受一定的算力供应商加入服务平台，并根据自身的任务特点，允许多种服务资源供应商加入平台[14-15]。同时，为了鼓励更多拥有高服务资源的算力供应商加入算力平台，算力平台将制定符合相应资源特点的合同奖励，以促进算力供应商的参与。

供应方单位服务成本组成成本主要由基本设施维护费用与供应商品功耗的额外增加量两部分组成。针对算力供应方商品，根据商品类型（计算资源、存储资源或网络资源）额外功耗有不同的衡量标准。

因此，根据其服务成本组成，可以获得算力供应方 j 获得的单位时间收入为：

$$p_{m,j}^{\mathrm{recv}} = p_{m,j}^{\mathrm{set}} \cdot g\left(\partial_{m,j}, \bar{e}_{m,j}\right) + R_n\left(\partial_n\right) - p_{m,j}^{\mathrm{cost}} \tag{11}$$

其中，$g\left(\partial_{m,j}, \bar{e}_{m,j}\right)$ 是根据平台客观评分以及交易合同中规定的 SLA 赔付标准构建的供应方收益折扣函数。算力平台提供包含一系列资源奖励包的合约 $(R_n(\partial_n), \partial_n)$ 给算力供应方。其中，$R_n(\partial_n)$ 为算力供应方相应的奖励。

算力供应方的目标（效用函数）是最大化其在算力资源商品服务供应中的单位利润。

$$\max_{\left(R_n, \partial_n\right)} u_{m,j}^{\mathrm{sup}} = \sum_{m=1}^{M} p_{m,j}^{\mathrm{recv}}, \forall m \in M \tag{12}$$

3.5　算力平台最优收益

考虑直接由用户和提供方完成算力服务定价与买卖的模式下，用户议价权低和交易并发量高时平台负载过重等关键因素。除了时延因素，算力供应方提供商品的综合质量评分也体现了客户的满意度，所以时延和质量评分都要被纳入算力平台收益模型。

考虑算力平台在资源交易的过程中不会进行额外盈利，可以认为算力平台代表用户群体的主要收益。

定义供应方 j、商品 m 的时延满意度：

$$\mathrm{sat}_{m,j}^{\mathrm{tran}} = \omega^{\mathrm{tran}} \ln\left(t^{\mathrm{tole}} - \overline{t_{m,j}^{\mathrm{tran}}}\right) \tag{13}$$

其中，$\omega^{\mathrm{tran}} > 0$ 为算力交易平台的时延满意度权重参数。在不失一般性的前提下，将 $\mathrm{sat}_{m,j}^{\mathrm{tran}}$ 表示为算力交易平台对供应方 j、商品 m 的传输时延的满意度函数。

定义供应方 j、商品 m 的综合评分满意度：

$$\mathrm{sat}_{m,j}^{\mathrm{sum}} = \omega^{\mathrm{sum}} \ln\left(\mathrm{e}_{m,j}^{\mathrm{sum}} - \mathrm{e}^{\mathrm{tol}}\right) \tag{14}$$

其中，$\omega^{\mathrm{sum}} > 0$ 为算力交易平台的综合评分满意度权重参数，$\mathrm{e}^{\mathrm{tol}}$ 为综合评分容忍值。在不失一般性的前提下，将 $\mathrm{sat}_{m,j}^{\mathrm{sum}}$ 表示为算力交易平台对供应方 j，商品 m 的综合评分满意函数。

算力平台代表用户，关于供应方商品的总收益为：

$$u_{m,j}^{\mathrm{plat}} = \mathrm{sat}_{m,j}^{\mathrm{tran}} + \mathrm{sat}_{m,j}^{\mathrm{sum}} + \mathrm{sat}_{m,j}^{\mathrm{pri}} - R_n\left(\partial_n\right) \tag{15}$$

算力平台希望在提供资源服务时最大化其收益。算力平台的总体目标是最大化所用供应资源的综合收益。

3.6　激励模型效果

在信息不对称的情况下，为了使合同可行，每个合同必须满足以下约束条件：个体合理性和激励兼容性，以确保每种类型的算力供应方得到充分的激励。根据博弈双方的最优效用，可构建最优收益优化问题：

$$\max_{\left(R_n, \partial_n\right)} \mathrm{sat}_{m,j}^{\mathrm{tran}} + \mathrm{sat}_{m,j}^{\mathrm{sum}} + \mathrm{sat}_{m,j}^{\mathrm{pri}} - R_n\left(\partial_n\right) \tag{16}$$

s.t.

$$p_{m,j}^{\mathrm{recv}} = p_{m,j}^{\mathrm{set}} \cdot g\left(\partial_{m,j}, \bar{e}_{m,j}\right) - p_{m,j}^{\mathrm{cost}} \geqslant 0$$

$$p_{m,j}^{\mathrm{set}} \cdot g\left(\partial_{m,j}, \bar{e}_{m,j}\right) - p_{m,j}^{\mathrm{cost}} \geqslant p_{l,j}^{\mathrm{set}} \cdot g\left(\partial_{l,j}, \bar{e}_{l,j}\right) - p_{l,j}^{\mathrm{cost}}$$

$$\overline{t_{m,j}^{\mathrm{tran}}} = \frac{1}{N_{m,j}^{\mathrm{tran}}} \sum_{i=1}^{N_{m,j}^{\mathrm{tran}}} t_{m,j}^{\mathrm{tran}} \leqslant t^{\mathrm{tole}}$$

$$\sum_{m=1}^{M} p_{m,j}^{\mathrm{set}} \leqslant p_m^{\mathrm{tole}}$$

基于以上模型设计，通过对个体合理和激励相容约束的迭代方法，借助凸优化方法可求得符合算力供应方与算力平台最大利益下的激励设计。针对求解得到的最优收益，本文进行了对应的效用收益仿真验证。

4　有效性验证

在图 6 中，通过评估信息不对称下激励机制的可行性，绘制了商品 1、商品 4、商品 7 和商品 10 的效用曲线。这些效用曲线清晰地表明，每种商品只有在选择与其相匹配的合约项目时才

能达到最大效用，从而验证了 IC 约束的有效性。

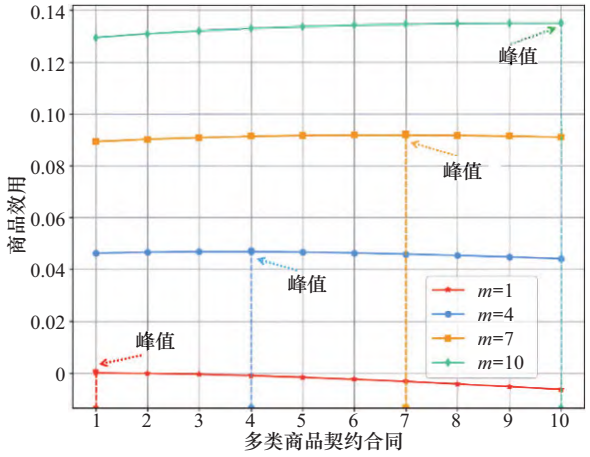

图6　最优收益仿真效果

Figure 6　Optimal profit simulation effect

图7显示，在基于最优契约合同的激励机制下，验证节点的总收益与供应方接受到的奖励均会随验证节点持有的资源商品的更替逐渐增高。高声誉的资源商品可以得到更高的社会福利。从而印证最优契约下，供应方契约合同收益的匹配性与收益单调性。

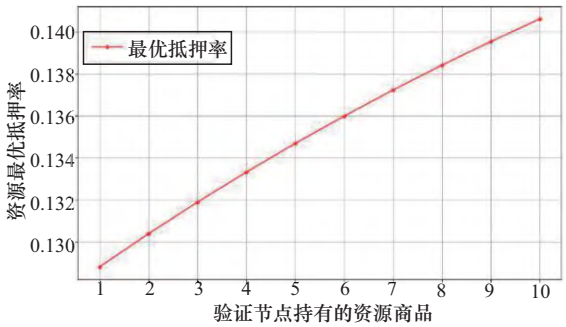

图7　节点资源最优抵押率折线

Figure 7　Line chart of optimal mortgage rate for node resources

图8描述了契约激励机制的效用单调性和动机效应。在本文的激励机制下，商品的总效用和奖励随着商品从1到10的变化而增加。例如，商品2的效用与奖励分别为0.0157和0.0268，商品10的效用和奖励分别为0.1349和0.1404，增加了759.2%和423.8%。激励机制可以鼓励供应商提高算网供应方服务可用性。

图9展示了本机制与不对称信息的性能。本文将其社会福利与具有完全信息激励、线性激励

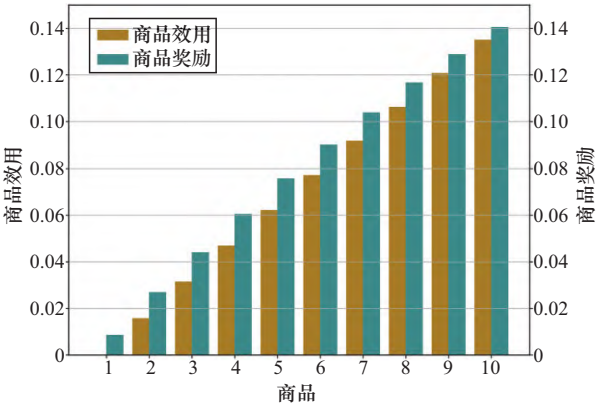

图8　商品效用及奖励

Figure 8　Product utility and reward

最优机制进行了比较[16-17]。图9表明，完全信息激励下的最优机制表现最好。以线性激励为例，本契约激励机制的平均社会福利为13.486比线性激励 γ=1.95 机制的平均社会福利13.275高1.58%。与完全信息激励与信托激励机制相比，本激励机制社会福利比完全信息激励机制的平均社会福利13.997低3.79%，比信托激励机制的平均社会福利13.663低1.31%，且随着商品增加，本机制与完全信息激励与信托激励机制下的社会福利差距会逐渐缩小。进一步可以观察到，随着商品的增加，具有完全信息的最优机制的社会福利将迅速下降，而本机制与具有完全信息的理想情况的差异将很小。

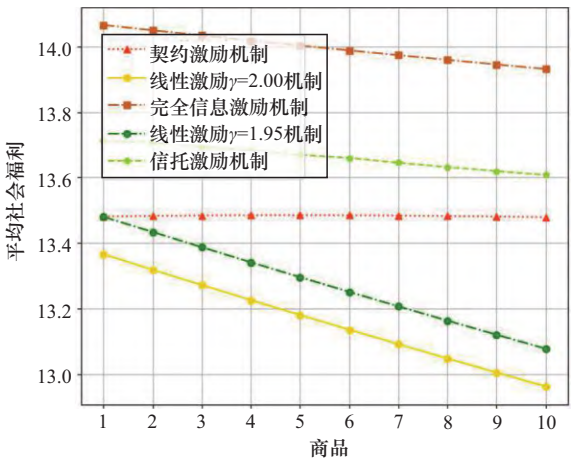

图9　节点资源平均社会福利收益折线

Figure 9　Line chart of average social welfare benefits for node resources

图10显示了本文的不对称信息激励机制的性能。本文将其平台效用于完全信息、线性激励

机制与信托激励机制的平台的最优效用进行了对比。观察到线性激励 γ=1.95 机制比线性激励 γ=2.00 机制表现更好。原因是调整因子代表的是单位奖励的能力，调整因子越小，平台支付的商品奖励越少。本契约激励机制的平台效用 13.414 比线性激励 γ=1.95 机制的平均平台效用 11.714 提高了 14.51%，其效用收益具有明显优势。与完全信息激励与信托激励机制相比，本机制的平均平台效用比完全信息激励机制的平均平台效用 13.997 低 4.17%，比信托激励机制的平均平台效用 13.654 低 1.76%，并且随着商品类型增加，本机制与完全信息激励与信托激励机制下的平均平台效用差距会逐渐缩小。

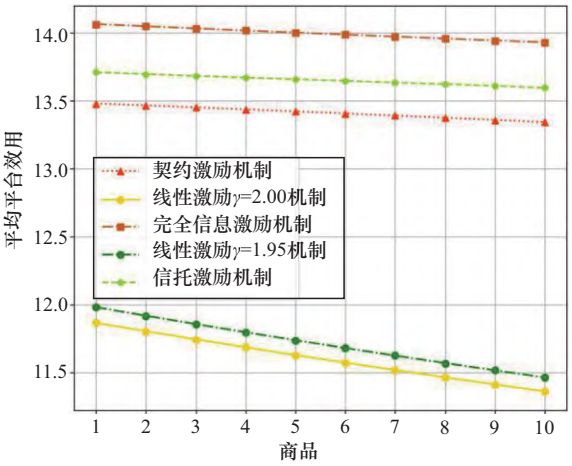

图 10　平均平台效用收益折线

Figure10　Average platform utility benefit line chart

5　结束语

为保证算力网络在弱信任或无信任的交易环境中完成可信交易，本文基于区块链与身份认证技术设计了可信身份管理与可信资源交易过程，保障了资源交易过程中的信息安全与身份可信。同时考虑供应方与平台用户的最优效用，在动态激励博弈模型下，构建了满足算力供应方基本收益和平台用户基本算力标准的交易激励模型，同时验证了本激励机制的可行性。

参考文献：

[1] 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.

[2] 程冠杰, 邓水光, 温盈盈, 等. 基于区块链的物联网认证机制综述[J]. 软件学报, 2023, 34(3): 1470-1490.
CHENG G J, DENG S G, WEN Y Y, et al. Survey on blockchain-based Internet of Things authentication mechanisms[J]. Journal of Software, 2023, 34(3): 1470-1490.

[3] 刘乃安, 陈智浩, 刘国堃, 等. 一种面向区块链验证节点的声誉证明共识机制[J]. 西安电子科技大学学报, 2020, 47(5): 57-62.
LIU N A, CHEN Z H, LIU G K, et al. Mechanism for proof of reputation consensus for blockchain validator nodes[J]. Journal of XIDIAN University, 2020, 47(5): 57-62.

[4] 李莉,周斯琴,刘芹,等.基于区块链的数字版权交易系统[J].网络与信息安全学报, 2018, 4(7): 22-29.
LI L, ZHOU S Q, LIU Q, et al. Blockchain-based digital copyright trading system[J]. Chinese Journal of Network and Information Security, 2018, 4(7): 22-29.

[5] 徐杨杨, 王艳. 区块链在云制造资源分配的研究[J]. 计算机科学与探索, 2022, 16(10): 2298-2309.
XU Y Y, WANG Y. Research on blockchain in cloud manufacturing resource allocation[J]. Journal of Frontiers of Computer Science and Technology, 2022, 16(10): 2298-2309.

[6] 袁勇, 王飞跃. 区块链技术发展现状与展望[J]. 自动化学报, 2016, 42(4): 481-494.
YUAN Y, WANG F Y. Blockchain: the state of the art and future trends[J]. Acta Automatica Sinica, 2016, 42(4): 481-494.

[7] 贾庆民,胡玉姣,张华宇,等.确定性算力网络研究[J].通信学报, 2022, 43(10): 55-64.
JIA Q M, HU Y J, ZHANG H Y, et al. Research on deterministic computing power network[J]. Journal on Communications, 2022, 43(10): 55-64.

[8] 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. Blockchain-based trust evaluation and guarantee scheme for computing power network[J]. Journal of Nanjing University of Posts and Telecommunications (Natural Science Edition), 2021, 41(4): 99-106.

[9] 张仕斌,许春香.基于云模型的信任评估方法研究[J].计算机学报, 2013, 36(2): 422-431.
ZHANG S B, XU C X. Study on the trust evaluation approach based on cloud model[J]. Chinese Journal of Computers, 2013, 36(2): 422-431

[10] 安宝怡. 开放系统环境下的可信移动群智感知数据交易机制研究[D]. 合肥: 中国科学技术大学, 2022.
AN B Y. Research on trustworthy mobile crowdsensing data trading mechanisms in open system circumstance[D]. Hefei: University of Science and Technology of China, 2022.

[11] 谢可, 余晗, 郝艳亚, 等. 基于可信数据的综合能源交易系统设计[J]. 电力信息与通信技术, 2019, 17(10): 44-48.
XIE K, YU H, HAO Y Y, et al. Design of integrated energy transaction system based on trusted data[J]. Electric Power Information and Communication Technology, 2019, 17(10): 44-48.

[12] 梁贺君, 韩景倜. 基于区块链的云计算资源去中心化交易共识机制研究[J]. 计算机科学, 2019, 46(S2): 548-552.
LIANG H J, HAN J T. Research on decentralized transaction consensus mechanism of cloud computing resources based on block chain[J]. Computer Science, 2019, 46(S2): 548-552.

[13] 唐飞, 包佳立, 黄永洪, 等. 基于属性的多授权中心身份认证方案[J]. 通信学报, 2021, 42(3): 220-228.
TANG F, BAO J L, HUANG Y H, et al. Multi-authority attribute-based identification scheme[J]. Journal on Communications, 2021, 42(3): 220-228.
[14] GUO W L, CHANG Z, GUO X J, et al. Incentive mechanism for edge computing-based blockchain: a sequential game approach[J]. IEEE Transactions on Industrial Informatics, 2019, 19(11): 7899-7909.
[15] 陈伟利, 郑子彬. 区块链数据分析: 现状、趋势与挑战[J]. 计算机研究与发展, 2018, 55(9): 1853-1870.
CHEN W L, ZHENG Z B. Blockchain data analysis: a review of status, trends and challenges[J]. Journal of Computer Research and Development, 2018, 55(9): 1853-1870.
[16] KANG J W, XIONG Z H, NIYATO D, et al. Incentive mechanism for reliable federated learning: a joint optimization approach to combining reputation and contract theory[J] IEEE Internet of Things Journal, 2021, 6(6): 10700-10714.
[17] WEN W, LU L, WANG W Z, et al. A contract-based incentive mechanism for resources trading in computing force networks[C]// Proceedings of the GLOBECOM 2023 - 2023 IEEE Global Communications Conference. Piscataway: IEEE Press, 2023: 5506-5511.

[作者简介]

张桂玉（1979– ），女，河南项城人，中讯邮电咨询设计院有限公司高级工程师，主要研究方向为智能云网技术机制。

刘博文（1993– ），男，河南郑州人，中讯邮电咨询设计院有限公司助理工程师，主要研究方向为数据骨干网相关技术。

梁晓晨（1988– ），男，北京人，中讯邮电咨询设计院有限公司工程师，主要研究方向为数据骨干网相关咨询设计与技术。

张笑颜（1997– ），女，河南驻马店人，中讯邮电咨询设计院有限公司工程师，主要研究方向为数据骨干网相关咨询设计与技术。

吕城锦（1991– ），男，山西吕梁人，中讯邮电咨询设计院有限公司工程师，主要研究方向为IP网规划和设计。

于思佳（1994– ），女，河南驻马店人，中讯邮电咨询设计院有限公司工程师，主要研究方向为数据网络、资源编排。

李硕（2000– ），男，安徽亳州人，北京邮电大学硕士生，主要研究方向为算力网络、区块链、可信交易。