计算机科学
COMPUTER SCIENCE

面向 6G 可信可靠智能的区块链分片与激励机制

王思明，谭北海，余荣

引用本文

王思明，谭北海，余荣. 面向 6G 可信可靠智能的区块链分片与激励机制[J]. 计算机科学, 2022, 49(6): 32-38.

WANG Si-ming, TAN Bei-hai, YU Rong. Blockchain Sharding and Incentive Mechanism for 6G Dependable Intelligence[J]. Computer Science, 2022, 49(6): 32-38.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.220400004

面向6G可信可靠智能的区块链分片与激励机制

王思明　谭北海　余　荣
广东工业大学自动化学院　广州 510006
(simingwang30@163.com)

摘　要　第六代(6G)无线通信网络将成为内生智能、泛在连接以及全场景互联互通的基座,是实现可信可靠智能的重要基础。区块链技术被认为是提升6G网络性能的去中心化赋能技术。未来区块链的共识节点将由海量边缘设备组成,并通过无线网络连接。然而,自利的边缘设备参与区块链共识过程仍面临着信息不完全对称、资源限制和异构无线通信环境的挑战。为此,提出了面向6G可信可靠智能的区块链分片与激励机制。为了最大化区块链分片的收益和可靠性,提出了基于实用拜占庭机制的区块链分片架构,同时设计了一个基于契约理论的激励机制。首先,通过分析基于实用拜占庭的片内共识机制及其区块在无线网络中的广播特性,构建了维护区块链分片网络的计算和通信的能耗模型;然后,为了提高系统可靠性和抵御恶意攻击的能力,提出了基于主观逻辑的信誉机制;最后,分别在信息完全对称和不完全对称的条件下求出了最优契约组合。该契约组合最大化区块链服务请求者的区块收益,同时满足预算可行性、个体理性和激励相容性。仿真结果表明,基于契约理论的激励机制能更可靠地激励边缘节点参与区块链共识过程,并从经济学角度有效地维护区块链的运行。

关键词:第六代无线通信网络;区块链分片;激励机制;契约理论;信誉机制
中图法分类号　TP393

Blockchain Sharding and Incentive Mechanism for 6G Dependable Intelligence

WANG Si-ming, TAN Bei-hai and YU Rong
School of Automation, Guangdong University of Technology, Guangzhou 510006, China

Abstract　The sixth generation(6G) wireless communication network will become the base of endogenous intelligence, ubiquitous connectivity, and full-scene interconnection. It is an important basis to realize dependable intelligence in the future. Blockchain is considered as the key decentralized-enabled technology to improve the performance of 6G networks. In the future, the consensus nodes of the blockchain will be composed of massive edge devices and connected through wireless networks. However, motivating self-interest edge devices to participate in the consensus process still faces the challenges of information asymmetry, resource constraints and heterogeneous wireless communication environment. To solve these challenges, a blockchain sharding framework and an incentive mechanism for trusted and dependable intelligence in 6G are proposed. Firstly, an incentive mechanism is presented based on contract theory, which aims to maximize the benefits and reliability of the blockchain sharding. By analyzing the practical byzantine fault tolerance (PBFT) based intrashard consensus mechanism, this paper design energy consumption model for auditing and transmitting the blocks in wireless networks. Secondly, in order to improve the system reliability, it proposes a reputation mechanism based on subjective logic. Finally, a set of optimal contracts under complete information and asymmetric information scnearios are abtained, which could optimize the block revenue for blockchain service requester, while ensuring some desired economic properties, i.e., budget feasibility, individual rationality and incentive compatibility. Simulation results show that the proposed contract-based incentive mechanism can motivate edge devices to participate in the blockchain consensus process and maintain the operation of blockchain from the perspective of economics more efficiently.

Keywords　6G, Blockchain sharding, Incentive mechanism, Contract theory, Reputation mechanism

1　引言

6G网络将在5G网络的基础上支持全场景的数字化,并结合区块链、人工智能等技术的发展,实现智慧的泛在连接、内生智能和全场景的互联互通[1-2]。在自动驾驶[3]、分布式账本[4]、数字孪生[5]和元宇宙[6]等应用方面,6G网络具有为

到稿日期:2022-04-01　返修日期:2022-04-29
基金项目:国家重点研发计划(2020YFB1807802,2020YFB1807800)
This work was supported by the National Key R&D Program of China(2020YFB1807802,2020YFB1807800).
通信作者:余荣(yurong@gdut.edu.cn)

人类提供泛在智能服务的巨大潜力，将极大地推动个人生活和社会经济的快速发展。

在未来 6G 网络中，物联网的快速发展使边缘设备数量激增，海量的边缘设备与数据中心之间频繁的数据传输会导致网络拥堵和过高的网络资源占用率[7]。此外，如何保障 6G 网络数据的安全性和隐私成为严峻的挑战。在 6G 网络中，海量边缘设备收集的数据可能包含敏感信息，大量的敏感数据暴露了传统的网络基础设施的数据安全隐患[8]。传统的网络基础设施往往是集中式的，这限制了 6G 网络的可扩展性。不仅如此，传统的网络基础设施容易遭受单点攻击，遭遇单点故障，且有隐私泄露的风险，会引发严重的数据安全问题[9]。现有的保护数据隐私安全和数据集中式处理的方法需要由第三方信任实体提供服务，边缘设备的数据需要由第三方实体进行处理。在这种情况下，海量的敏感数据可能面临着被滥用和隐私泄露的风险。

区块链作为一种可追溯、去中心化、不可篡改的分布式账本，近年来受到学术界和工业界的关注[7]。区块链建立在对等网络之上，依赖分布式节点之间的交互和通信来维护一个共同的账本。共识机制在区块链中起着关键作用，它确保了交易的顺序以及区块链数据的完整性和一致性。区块链的共识机制决定了区块链的安全边界和其他关键性能指标，如交易吞吐量、延迟和可扩展性[8]。但是，由于边缘设备的资源限制和无线通信网络环境不稳定，传统的区块链应用无法直接部署到边缘设备上。大多数传统的区块链应用都依赖于理想的假设，即区块链参与者拥有无限的能源供应和稳定的数据传输环境。然而，这些假设在边缘网络中是不现实的，因为海量的边缘设备通常面临着计算和通信资源的限制以及复杂的无线通信环境的挑战[9]。

为了解决上述问题，本文提出了面向 6G 可信可靠的区块链分片与激励机制。考虑到边缘设备异构的计算和通信环境以及边缘设备与区块链服务请求者之间的信息不完全对称，设计了基于契约理论的激励机制。此外，本文设计了一个基于实用拜占庭共识机制的区块链分片架构。通过分析区块在无线网络的广播特性和校验区块的损耗，建立了面向区块链分片共识机制的计算和通信的能耗模型。为了提高区块链分片系统的可靠性，本文提出了基于主观逻辑的信誉机制。最后，本文分别在信息完全对称和不完全对称的条件下求解了最优契约组合。该契约组合最大化区块链服务请求者的区块收益，同时满足预算可行性、个体理性和激励相容性约束。仿真结果表明，本文提出的基于契约理论的激励机制能更可靠地激励边缘设备参与区块链分片的共识过程。

本文第 2 节回顾了相关工作；第 3 节建立了区块链分片的系统模型，构建了边缘设备在区块链共识过程的能耗模型；第 4 节论证了契约理论的可行条件，并设计了目标函数和求解方法；第 5 节给出了验证契约可行性的仿真结果；最后总结全文。

2 相关工作

在现有的区块链激励机制工作中，Jiao 等[10]为了保持区块链数据记录的规范状态，针对公有链的基于工作量证明的共识协议，为网络中的节点提供激励。他们专注于雾计算服务商与节点之间的交易，并提出了一种基于拍卖的市场模型，用于高效地计算资源分配。Yang 等[11]针对现有共识算法存在效率低下和缺少激励机制等问题，提出了一种基于演化博弈的理性实用拜占庭容错共识算法。首先，通过引入信誉机制来确定节点在共识过程中的可信任度，以信誉值为理性节点共识积极性的依据，基于信誉对共识节点进行划分，采用节点网络分片化的共识方式来提升共识效率。其次，针对共识过程中节点之间链路动态性对信誉值产生的影响建立演化博弈模型，并证明信誉稳定策略存在纳什均衡，设计基于信誉稳定策略的激励机制，以提升共识节点参与共识过程的积极性。Wang 等[12]主要研究了在无线传感网络中的区块链部署，考虑到物联网设备之间的异构能力和无线传感网络中的信息不完全对称，设计了一个多维合约来激励无线传感节点，以维护区块链。该契约方案考虑到无线传感器的能量有限，改进了比特币的区块传播协议并比较了两种协议。

在区块链分片的激励机制方面，Li 等[13]在异构物联网场景下提出了两个基于契约理论的联合模型，旨在根据参与者的保证金和表现（努力）来确定参与者的奖励。与以太坊 2.0 中的安全激励相比，提议的两种模型能够平衡信标链和参与者的安全激励和经济激励。这两个模型将拥有物联网设备的任何个人和机构都视为潜在参与者，并重点在具有隐藏信息和隐藏动作的实际场景中设计适当的保证金。Li 等[14]利用契约理论和斯坦伯格博弈在分层博弈的框架下设计了区块链分片的网络保险机制，并提出了一种通过整合网络保险理念来中和网络风险的激励方案，确定不同验证者的退出延迟，并为其损失提供保险索赔。这意味着区块链系统可以通过合同中确定的“延迟”来保留更多的在线存款以抵抗威吓攻击。Manshaei 等[15]针对区块链分片的共识协议设计激励机制。这些激励措施将促进分片内部的合作并防止搭便车攻击。Chen 等[16]研究了如何在基于分片的区块链中正确分配用户，以提升系统交易性能。首先建立了一个开放的杰克逊排队网络模型以捕捉用户在分片上的交易动态，然后将用户的交互视为基于分片的区块链博弈，其中每个用户的目标是最小化其交易确认时间和交易费用。Chen 等研究了博弈的均衡，并设计了一种多项式时间算法来找到具有良好系统性能的有效均衡。

3 系统框架和模型建立

3.1 系统框架

如图 1 所示，面向 6G 可信可靠的区块链分片系统包括区块链层和应用层。在区块链层，区块链的主链部署在边缘服务器中，分片区块链则部署在边缘设备中。为了有效地处理来自边缘网络的海量数据，区块链分片系统用于以并行方式处理大量交易。首先，区块链共识节点被分配到不同的分片中，不同的分片独立地创建区块，并通过分片内的共识机制来验证区块的合法性和完整性。其次，在每个分片中创建的区块通过分片间最终的共识再次合并和验证。

最后，将新的区块加入主链中。

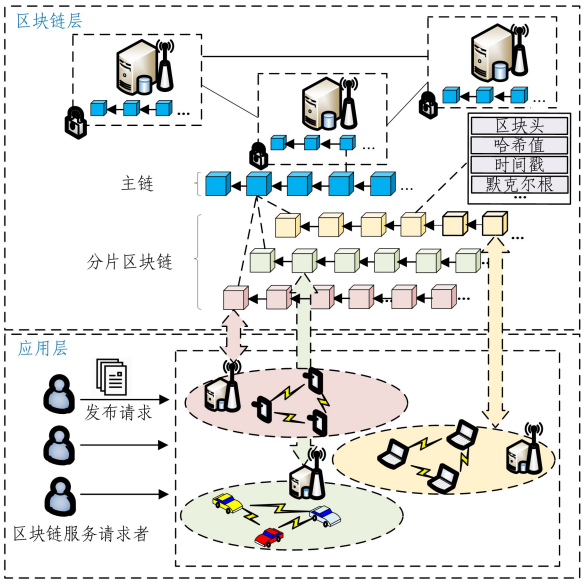

图 1 系统模型

Fig. 1 System model

在应用层，区块链服务请求者希望在边缘网络中确保数据共享和数据交易的安全管理。但是，边缘设备参与区块链共识机制需要付出大量的通信和计算能耗，自利的边缘设备通常不愿意参与其中。区块链服务请求者与边缘节点存在着信息不完全对称的问题，即请求者不了解边缘节点的硬件特性和通信环境，无法为边缘节点制定合适的激励方案。契约理论是一种专门用于解决信息不完全对称问题的经济学工具，被广泛应用于无线通信领域的研究[13-14]。为了区块链分片系统的部署，区块链服务请求者可以设计契约组合来激励边缘设备参与区块链分片的共识机制，其目标是最大化区块收益，而边缘设备的目标是最大化自身的效用。

3.2 信誉模型

在面向 6G 网络的区块链系统中，为了提高系统可靠性和抵御恶意攻击的能力，在区块链共识过程中应该更信赖信誉度高的节点。本文综合考虑了节点的历史行为对信誉值的影响。

考虑在离散的时间周期 $T=\{1,2,\cdots,t,\cdots\}$ 上，区块链分片系统中存在一组边缘节点，用集合 $\Lambda=\{1,2,\cdots,m,\cdots,M\}$ 表示。在拜占庭攻击中，恶意节点可能会发起不正确投票或不投票行为。因此，引入了恶意攻击的交互记录，以削弱恶意节点的威胁。基于主观逻辑模型[17]，节点 m 对节点 n 在时隙 t 的评价可以表示为：

$$h_{m\to n}^{t}=(1-u_{m\to n}^{t})\cdot\frac{\alpha_{m}^{t}}{\alpha_{m}^{t}+\beta_{m}^{t}} \tag{1}$$

其中，α_{m}^{t} 是积极的交互次数；β_{m}^{t} 是恶意的行为次数，如故意投错票或者不投票等行为。节点 m 对于节点 n 的信誉值可表示为：

$$g_{m\to n}=\sum_{t=1}^{T}(h_{m\to n}^{t}+\sigma u_{m\to n}^{t}) \tag{2}$$

其中，σ 是一个系数，表示不确定性的影响程度，$u_{m\to n}^{t}$ 表示数据包传输的失败概率。节点 n 的平均信誉值可以表示为：

$$g_{n}=\frac{\sum_{m=1}^{M}g_{m\to n}}{M} \tag{3}$$

区块链服务请求者会选择信誉值较高的节点，以提高系统的可靠性。当节点的信誉值大于阈值时，$g_{n}\geqslant g_{th}$，则该节点是可信的，将会被选择成为候选的共识节点，否则，该边缘节点不可信。

3.3 能耗模型

通过信誉值筛选后，候选的共识节点在分片区块链系统中被分配到多个分片中。分片用集合 $\Gamma=\{1,2,\cdots,i,\cdots,I\}$ 表示。分配到第 i 个分片的多个边缘节点将被分成多个类型，用集合 $\Phi=\{1,2,\cdots,j,\cdots,J\}$ 表示。边缘节点具有异构的计算资源、通信资源和无线传输环境。分片中的边缘节点可按一定的方法进行分类，如通过历史数据统计等。

在区块链分片的共识过程中，边缘节点的能耗主要由区块传输的通信能耗和计算能耗组成。如图 2 所示，分片区块链采用的共识协议基于实用拜占庭共识协议，图中描述了片内的共识机制。分片内的共识节点经过了信誉值的筛选，分片间的共识机制由共识节点选举出来的节点委员会执行，可参考文献[18]。在分片内的共识机制中，每个共识节点共识一个区块时需要接收和转发多次区块。片内共识节点共识一个区块的能耗如下：

$$E_{i,j}=\mu\left(\frac{s}{r_{i,j}^{tx}}P_{i,j}^{tx}+\frac{s}{r_{i,j}^{rx}}P_{i,j}^{rx}+c\kappa_{i,j}f_{i,j}^{2}\right) \tag{4}$$

其中，μ 是边缘节点在分片内共识一个区块需要转发和校验区块的次数；s 为区块的大小；$r_{i,j}^{tx}$ 和 $r_{i,j}^{rx}$ 分别为发送速率和接收速率；$P_{i,j}^{tx}$ 和 $P_{i,j}^{rx}$ 分别为发送功率和接收功率；c 是校验一个区块的计算复杂度，包括验证签名和消息认证码操作；$\kappa_{i,j}$ 表示边缘节点的电容开关参数，与边缘节点的硬件特性有关；$f_{i,j}$ 表示边缘节点的计算能力。

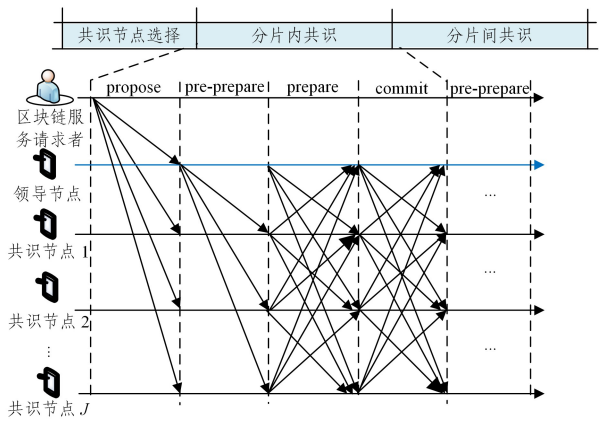

图 2 基于实用拜占庭容错的分片内共识机制

Fig. 2 Intrashard consensus mechanism based on practical Byzantine fault tolerance

3.4 边缘节点和区块链服务请求者的效用函数

第 i 个分片的第 j 个类型的节点的效用函数可被定义为收入的报酬减去区块链共识过程中的计算和通信能耗，表示为：

$$V_{i,j}=\pi_{i,j}-eE_{i,j}b_{i,j}=\pi_{i,j}-\frac{b_{i,j}}{\phi_{i,j}} \tag{5}$$

其中，$\pi_{i,j}$ 为边缘节点的报酬，e 为能耗与金钱的转化参数，$b_{i,j}$ 为区块的数量，$\phi_{i,j}=1/eE_{i,j}$ 被定义为第 i 个分片的第 j 类节点的类型。

区块链服务请求者的效用函数可被定义为满意度的收益减去付出的报酬。对于第 i 个分片的第 j 个类型的节点，效用函数可定义为：

$$U_{i,j}=\rho\log(1+g_{i,j}b_{i,j})-\pi_{i,j} \tag{6}$$

其中，$g_{i,j}$ 是第 i 个分片的第 j 个类型节点的平均信誉值，ρ 是单位满意度的利润系数。式(6)的满意度函数随着区块数 $b_{i,j}$ 的增加而增大，增加的速率逐渐递减。

3.5 契约制定的可行性约束

为了激励边缘节点参与到区块链分片的共识过程中，基于契约理论的激励机制需要满足个体理性和激励相容性约束。契约的个体理性约束确保边缘节点的效用大于零。不但解决边缘节点与区块链服务请求者的信息不完全对称的问题，还应保证激励相容性得到满足[19]。激励相容性约束确保每个类型的边缘节点只有在签署为其实际类型制定的契约时才能实现最大效用，以确保边缘节点会按照真实情况选择相应的契约，即向区块链服务请求者如实报告其类型[20]。

定义 1(个体理性) 个体理性保证所有参与区块链共识的边缘节点效用函数为非零，记作：

$$V_{i,j}\geqslant 0, i\in I, j\in J \tag{7}$$

定义 2(激励相容性) 激励相容性保证参与区块链共识的每个边缘节点仅在以下条件下获得最大效用：

$$V_{i,j}\geqslant V_{i,j'}, i\in I, j, j'\in J \tag{8}$$

定义 3(预算可行性) 预算可行性确保所有参与区块链共识的边缘节点的总报酬不超过预算 B，记作：

$$\sum_{j\in J}\gamma_{i,j}\pi_{i,j}\leqslant B \tag{9}$$

其中，$\gamma_{i,j}$ 是第 i 个分片的第 j 个类型边缘节点的比例，满足 $\sum_{j\in J}\gamma_{i,j}=1$。

4 目标函数的构建和解决方法

4.1 信息完全对称的最优解

在信息完全对称的条件下，区块链服务请求者预先知道每个边缘节点的类型，可以专门为每个类型的节点设计和提供与其类型对应的一份契约。请求者只需要考虑预算可行性和个体理性。假设有 N 个边缘节点参与到共识过程中，综上所述，信息完全对称的最优契约设计可表述为：

$$\begin{aligned}&\max_{(b_{i,j},\pi_{i,j})}\ \sum_j N\gamma_{i,j}[\rho\log(1+g_{i,j}b_{i,j})-\pi_{i,j}]\\&\text{s.t. C1}:\pi_{i,j}-\frac{b_{i,j}}{\phi_{i,j}}\geqslant 0,\ \forall j\in J\\&\quad\text{C2}:\sum_j\gamma_{i,j}\pi_{i,j}\leqslant B\end{aligned} \tag{10}$$

首先将问题(10)简化，如引理 1 和引理 2 所述。

引理 1 问题(10)的个体理性约束可简化成等式的约束，如 $\pi_{i,j}-b_{i,j}/\phi_{i,j}=0$。

证明：假设存在一个最优契约，它为第 j 个类型中的节点提供效用 $\pi_{i,j}-b_{i,j}/\phi_{i,j}>0$，但区块链服务请求者只需满足边缘节点的个体理性。因此，区块链服务请求者总是可以选择更大的 $b_{i,j}$ 来提高自己的满意度，直到 $\pi_{i,j}-b_{i,j}/\phi_{i,j}=0$。

引理 2 问题(10)的预算可行约束可简化为等式约束，如 $\sum_{j\in J}\gamma_{i,j}\pi_{i,j}=B$。

证明：如果一组契约满足 $\sum_{j\in J}\gamma_{i,j}\pi_{i,j}<B$，服务请求者总是可以选择更大的 $\pi_{i,j}$ 以获取更大的 $b_{i,j}$ 并提高自身的满意度，直到满足 $\sum_{j\in J}\gamma_{i,j}\pi_{i,j}=B$。

根据引理 1 和引理 2，优化问题(10)可等效地转化为：

$$\begin{aligned}&\max_{(b_{i,j},\pi_{i,j})}\ \sum_j N\gamma_{i,j}[\rho\log(1+g_{i,j}b_{i,j})-\pi_{i,j}]\\&\text{s.t. C1}:\pi_{i,j}-\frac{b_{i,j}}{\phi_{i,j}}=0,\ \forall j\in J\\&\quad\text{C2}:\sum_j\gamma_{i,j}\pi_{i,j}=B\end{aligned} \tag{11}$$

与问题(10)相比，问题(11)可轻易地通过 Karush-Kuhn-Tucker (KKT) 条件下的拉格朗日分析来解决。

4.2 信息不完全对称的最优求解

与信息完全对称相比，信息不完全对称更接近现实的情况。在信息不完全对称的条件下，区块链服务请求者仅知道边缘节点的类型分布。为了克服信息不完全对称，区块链服务请求者需要向每个类型的边缘节点发布所有类型的契约。因此，除了预算可行性和个体理性的约束，契约还必须满足激励相容性约束。区块链服务请求者的效用最大化问题可描述如下：

$$\begin{aligned}&\max_{(b_{i,j},\pi_{i,j})}\ \sum_j N\gamma_{i,j}[\rho\log(1+g_{i,j}b_{i,j})-\pi_{i,j}]\\&\text{s.t. C1}:\pi_{i,j}-\frac{b_{i,j}}{\phi_{i,j}}\geqslant 0,\ \forall j\in J\\&\quad\text{C2}:\pi_{i,j}-\frac{b_{i,j}}{\phi_{i,j}}\geqslant\pi_{i,j'}-\frac{x_{i,j'}}{\phi_{i,j}},\ \forall j, j'\in J\\&\quad\text{C3}:\sum_j\gamma_{i,j}\pi_{i,j}=B\end{aligned} \tag{12}$$

问题(12)有 J 个个体理性约束和 $J*(J-1)$ 个激励相容约束，因此求解问题(12)变得非常复杂。问题(12)的约束简化过程将在下面的引理中详细阐述。

引理 3 问题(12)的个体理性约束可简化为：

$$\pi_{i,0}-\frac{b_{i,0}}{\phi_{i,0}}\geqslant 0,\ \forall i\in I \tag{13}$$

证明：已知 $\phi_{i,1}<\phi_{i,2}<\cdots<\phi_{i,J}$，根据激励相容约束，可以得到：

$$\pi_{i,j}-\frac{b_{i,j}}{\phi_{i,j}}\geqslant\pi_{i,1}-\frac{b_{i,1}}{\phi_{i,j}}>\pi_{i,1}-\frac{b_{i,1}}{\phi_{i,1}} \tag{14}$$

如式(14)所示，最低类型的节点获得最低的效用。因此，如果设计的契约组合能够确保最低类型的节点获得非负的效用，则所有类型节点的个体理性约束都能得到保证。

引理 4 问题(12)的个体理性约束和预算可行约束可以简化成等式的约束，如 $\pi_{i,j}-b_{i,j}/\phi_{i,j}=0$ 和 $\sum_{j\in J}\gamma_{i,j}\pi_{i,j}=B$。

证明：这里省略证明，因为其类似于引理 1 和引理 2 的证明。

引理 5(单调性) 契约组合将为高类型的节点提供更高的报酬。对于任何两个可行的契约，如果 $b_{i,j}\geqslant b_{i,j'}$，则 $\pi_{i,j}\geqslant\pi_{i,j'}$。

证明：根据激励相容约束，可得：

$$\pi_{i,j}-b_{i,j}/\phi_{i,j}\geqslant\pi_{i,j'}-b_{i,j'}/\phi_{i,j} \tag{15}$$

$$\pi_{i,j'}-b_{i,j'}/\phi_{i,j'}\geqslant\pi_{i,j}-b_{i,j}/\phi_{i,j'} \tag{16}$$

将式(15)和式(16)相加，可得：

$$(b_{i,j'}-b_{i,j})(1/\phi_{i,j}-1/\phi_{i,j'})\geqslant 0 \tag{17}$$

由式(17)可知，若 $\phi_{i,j}\geqslant\phi_{i,j'}$，则 $b_{i,j}\geqslant b_{i,j'}$。

基于引理5单调性的性质，本文将尝试简化问题(12)的激励相容约束。首先介绍以下两个性质：局部向下激励相容性和局部向上激励相容性。

$$\pi_{i,j}-b_{i,j}/\phi_{i,j}\geqslant\pi_{i,j-1}-b_{i,j-1}/\phi_{i,j} \tag{18}$$

$$\pi_{i,j}-b_{i,j}/\phi_{i,j}\geqslant\pi_{i,j+1}-b_{i,j+1}/\phi_{i,j} \tag{19}$$

利用上述局部向下激励相容性和局部向上激励相容性，激励相容约束可进一步简化。

引理6 如果满足局部向下激励相容约束，则问题(12)的激励相容约束可得到满足。

证明：根据 $\phi_{i,1}<\phi_{i,2}<\cdots<\phi_{i,J}$ 和引理5，可以得到：

$$\begin{aligned}&\pi_{i,j-1}-b_{i,j-1}/\phi_{i,j-1}\geqslant\pi_{i,j-2}-b_{i,j-2}/\phi_{i,j-1}\\&\Rightarrow\pi_{i,j+1}-\pi_{i,j-2}\geqslant(b_{i,j-1}-b_{i,j-2})/\phi_{i,j-1}\\&\Rightarrow\pi_{i,j-1}-\pi_{i,j-2}\geqslant(b_{i,j-1}-b_{i,j-2})/\phi_{i,j}\\&\Rightarrow\pi_{i,j-1}-b_{i,j-1}/\phi_{i,j}\geqslant\pi_{i,j-2}-b_{i,j-2}/\phi_{i,j}\end{aligned} \tag{20}$$

根据局部向下激励相容约束，可得：

$$\pi_{i,j}-b_{i,j}/\phi_{i,j}\geqslant\pi_{i,j-1}-b_{i,j-1}/\phi_{i,j} \tag{21}$$

根据式(20)和式(21)，可得：

$$\pi_{i,j}-b_{i,j}/\phi_{i,j}\geqslant\pi_{i,j-2}-b_{i,j-2}/\phi_{i,j}>\cdots>\pi_{i,1}-b_{i,1}/\phi_{i,j} \tag{22}$$

用类似的方法，可得：

$$\pi_{i,j}-b_{i,j}/\phi_{i,j}\geqslant\pi_{i,j+2}-b_{i,j+2}/\phi_{i,j}>\cdots>\pi_{i,J}-b_{i,J}/\phi_{i,j} \tag{23}$$

根据式(22)和式(23)，激励相容约束可全部满足。

引理7 局部向上激励相容约束和局部向下激励相容约束可以化简为等式约束，记作：

$$\pi_{i,j}-b_{i,j}/\phi_{i,j}=\pi_{i,j-1}-b_{i,j-1}/\phi_{i,j} \tag{24}$$

证明：用反证法来证明引理7。假设局部向上激励相容约束在当前的契约不满足，即 $\pi_{i,j}-b_{i,j}/\phi_{i,j}>\pi_{i,j-1}-b_{i,j-1}/\phi_{i,j}$。根据引理5和引理6可得到 $\pi_{i,j}-b_{i,j}/\phi_{i,j}\geqslant\pi_{i,1}-b_{i,1}/\phi_{i,j}\geqslant\pi_{i,1}-b_{i,1}/\phi_{i,1}=0$。在不违反任何约束的情况下，服务请求者可以通过增加 $b_{i,j}$ 来获得更好的效用，直到等式满足。

然后，根据局部向上激励相容约束，可以得到：

$$\begin{aligned}&\pi_{i,j-1}-b_{i,j-1}/\phi_{i,j-1}=\pi_{i,j}-b_{i,j}/\phi_{i,j-1}\\&\Rightarrow\pi_{i,j-1}-\pi_{i,j}=(b_{i,j-1}-b_{i,j})/\phi_{i,j-1}\\&\Rightarrow\pi_{i,j-1}-\pi_{i,j}\geqslant(b_{i,j-1}-b_{i,j})/\phi_{i,j}\\&\Rightarrow\pi_{i,j}-b_{i,j}/\phi_{i,j}\geqslant\pi_{i,j-1}-b_{i,j-1}/\phi_{i,j}\end{aligned} \tag{25}$$

因此，根据定理4－定理7，问题(12)可以简化为：

$$\begin{aligned}&\max_{(b_{i,j},\pi_{i,j})}\ \sum_j N\gamma_{i,j}[\rho\log(1+g_{i,j}b_{i,j})-\pi_{i,j}]\\&\text{s.t. C1}:\pi_{i,1}-\frac{b_{i,1}}{\phi_{i,1}}=0\\&\quad\text{C2}:\pi_{i,j}-\frac{b_{i,j}}{\phi_{i,j}}=\pi_{i,j-1}-\frac{b_{i,j-1}}{\phi_{i,j}},\forall j\in J\\&\quad\text{C3}:\sum_j\gamma_{i,j}\pi_{i,j}=B\end{aligned} \tag{26}$$

根据问题(26)的C1和C2约束，可得：

$$\begin{aligned}\pi_{i,j}&=\frac{b_{i,1}}{\phi_{i,1}}+\sum_{k=2}^{j}\frac{b_{i,k}-b_{i,k-1}}{\phi_{i,k}}\\&=\frac{b_{i,j}}{\phi_{i,j}}+\sum_{k=2}^{j}\left(\frac{1}{\phi_{i,k-1}}-\frac{1}{\phi_{i,k}}\right)b_{i,k-1},k\in\{2,3,\cdots,J\}\end{aligned} \tag{27}$$

使用式(27)替换问题(26)的 $\pi_{i,j}$，可得：

$$\begin{aligned}&\max_{b_{i,j}}\sum_j N\gamma_{i,j}[\rho\log(1+g_{i,j}b_{i,j})]-\sum_j\delta_{i,j}b_{i,j}\\&\text{s.t. C1}:\sum_j\delta_{i,j}b_{i,j}=B\end{aligned} \tag{28}$$

其中，

$$\delta_{i,j}=\begin{cases}\dfrac{1}{\phi_i}\sum\limits_{j=i}^{J}N\gamma_{i,j}-\dfrac{1}{\phi_{i+1}}\sum\limits_{j=i+1}^{J}N\gamma_{i,j}, & 1\leqslant j<J\\\dfrac{N\gamma_{i,J}}{\phi_{i,J}}, & j=J\end{cases} \tag{29}$$

与原始问题相比，简化的优化问题(29)可通过KKT条件下的拉格朗日分析来解决。优化问题的对应拉格朗日等式为：

$$L=\sum_j N\gamma_{i,j}\rho\log(1+g_{i,j}b_{i,j})-\sum_j\delta_{i,j}b_{i,j}+\phi\sum_j\delta_{i,j}b_{i,j}-\phi B \tag{30}$$

其中，ϕ 是朗格朗日乘子。基于KKT条件，将拉格朗日等式关于 $b_{i,j}$ 和 ϕ 的一阶导数设为零，经过推导，得到了最优契约的解，如式(31)所示：

$$b_{i,j}^{*}=N\gamma_{i,j}\rho\Big/\left(\frac{\sum N\gamma_{i,j}\rho}{B+\sum_j\delta_{i,j}/g_{i,j}}\right)\delta_{i,j}-1/g_{i,j} \tag{31}$$

根据激励相容约束和式(27)，可得：

$$\pi_{i,j}^{*}=\frac{\delta_{i,j}b_{i,j}^{*}}{\gamma_{i,j}} \tag{32}$$

此外，如果求解出来的契约组合不满足引理5的单调性，则可以使用子序列替换算法来解决单调性的问题[21]。在边缘节点类型均匀分布的情况下，契约组合正好处于递增顺序。但是，在边缘节点类型一般分布的情况下，契约组合可能不是按递增顺序排列的。契约组合有可能是不可行的，需要进行调整。

5 实验分析

基于仿真实验，本文首先分析了契约的可行性；然后研究了预算和区块尺寸对区块链服务请求者和边缘节点效用的影响；最后研究了信誉阈值对区块链服务请求者效用的影响。仿真参数设置如下，本文考虑了30个边缘节点，3个分片，每个分片包含10种类型。本文假设边缘节点类型服从均匀分布，节点之间总的交互次数均匀分布于[100，200]，节点发起攻击的概率均匀分布于[0，1]。具体的仿真参数设置如表1所列[10,18]。

表1 仿真参数

Table 1 Simulation parameters

参数	值	参数	值
$f_{i,j}$/GHz	[8，10]	s/Mbit	64
$r_{i,j}^{tx},r_{i,j}^{rx}$/(Mbit/s)	[10，20]	c/MHz	38
$P_{i,j}^{tx},P_{i,j}^{rx}$/W	[0.1，0.2]	ρ	10^4
$\kappa_{i,j}$	$[10^{-28},10^{-27}]$	e	1
$u_{m\to n}^{t}$	[0，1]	B	5000

为了验证在信息不完全对称条件下基于契约理论的激励方案的个体理性和激励相容约束，本文首先给出了为相应类型节点设计的效用函数。图3给出了在信息不完全对称条件下的类型7、类型8和类型9的边缘节点效用。可以看出，类型越高的节点的效用越大。当每种类型的节点选择其对应类型的契约时，它的效用函数达到最大值，这表明了在信息不完全对称的情况下的最优求解是满足激励相容约束的。此外，每种类型的节点选择相应的契约后，它的效用值均大于0，这表明求解的契约组合满足个体理性。因此，通过应用提出的

基于契约理论的激励方案，服务请求者可以获得节点的隐私偏好，从而解决信息不完全对称的问题。

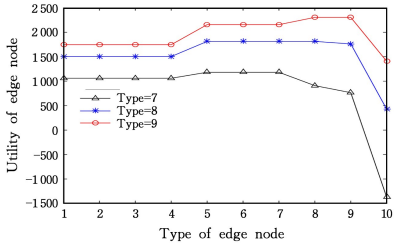

图 3　边缘节点的效用与节点的类型比较

Fig. 3　Utility of edge node versus type of edge node

为了研究系统预算对所提契约方案的影响，图 4 给出了 3 种方案下区块链服务请求者的效用与预算的比较。由图 4 可知，随着预算的增加，服务请求者都能实现更高的效用，原因是当区块链服务请求者增加更多的预算时，它可以提供更多的报酬来激励边缘节点在单位时间内共识更多的区块，这有利于提高区块链网络的效率。在 3 种策略中，红色线表示的信息完全对称方案最优，能够在任何预算下产生最多的效用，这是因为信息完全对称方案了解所有节点的隐私偏好，让边缘节点保持零效用。蓝色线表示的信息不完全对称的方案比黑色线表示的同一契约方案更好，这是因为信息不完全对称方案为边缘节点不同类型的专属设计，满足激励相容性，所以信息不完全对称的方案比同一契约的方案更好。

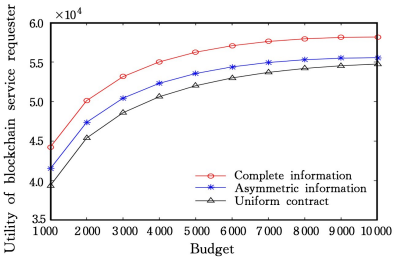

图 4　3 种方案下区块服务请求者的效用与预算的比较（电子版为彩图）

Fig. 4　Utility of blockchain service requester versus budget with three schemes

图 5 给出了 3 种策略下边缘节点的效用与预算的比较。可以看出，随着预算的增加，除了信息完全对称方案保持零效用外，其他两种方案的边缘节点效用都有所提高。这是因为信息完全对称方案了解所有节点的隐私偏好，使边缘节点保持零效用。当区块链服务请求者增加更多的预算时，边缘节点可获得更多的报酬，从而在单位时间内共识更多的区块。

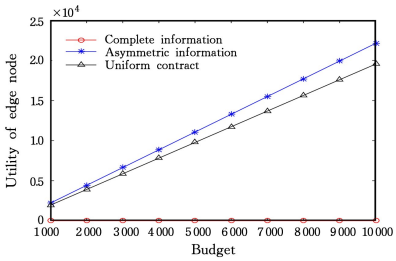

图 5　3 种方案下边缘节点的效用与预算的比较

Fig. 5　Utility of edge node versus budget with three schemes

为了研究区块尺寸对区块链服务请求者效用的影响，图 6 给出了 3 种策略下区块链服务请求者的效用与区块尺寸的比较。如图 6 所示，随着区块的尺寸增加，区块链服务请求者的效用降低。这是因为当区块尺度增加时，共识单位区块的通信和计算的能耗也相应地增加，这影响了区块链出块的效率。与图 4 类似，信息完全对称的方案为区块链服务请求者带来了最大的效用，其次是信息不完全对称的方案。在信息不完全对称的场景下，激励相容性的设计只能为服务请求者带来近似的最优效用。信息完全对称方案可作为上界。与其他两种方案相比，同一契约的性能最差。

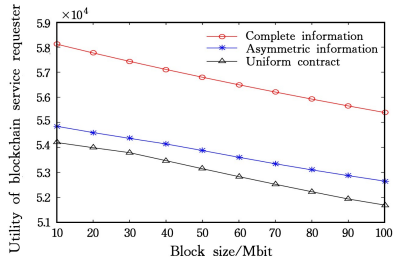

图 6　3 种方案下区块链服务请求者的效用与区块尺寸的比较

Fig. 6　Utility of blockchain service requester versus size of block

图 7 给出了边缘节点效用在不同策略下随区块尺寸变化的性能图。可以看出，随着区块尺寸的增加，除了信息完全对称方案保持零效用外，其他两种方案的边缘节点效用都有所减少。其原因与图 4 中的结果产生的原因类似。在信息完全对称的模型下，服务请求者了解所有类型节点的隐私信息，只需满足节点的个体理性即可。因此，服务请求者获得了所有效用。在信息完全对称的条件下，由于激励相容性的约束，服务请求者需要付出更多的报酬来解决信息不完全对称的问题。因此，节点获得的效用比信息完全对称更大。

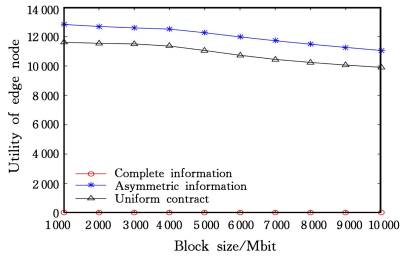

图 7　3 种方案下边缘节点效用与区块尺寸的比较

Fig. 7　Utility of edge node versus size of block

为了研究不同的信誉阈值对区块链服务请求者效用的影响，图 8 给出了 3 种阈值下区块链服务请求者的效用与边缘节点类型的比较。

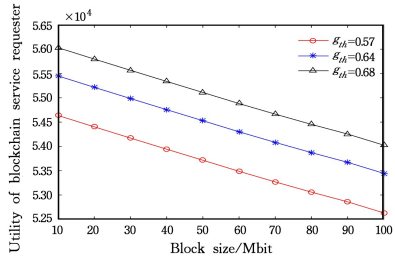

图 8　不同信誉阈值下区块链服务请求者效用与区块尺寸的比较

Fig. 8　Utility of blockchain service requester versus block size with different reputation threshold

如图 8 所示，随着区块尺寸的增加，区块链服务请求者的效用相应减少。另外，随着信誉阈值的增加，区块链服务请求者的效用越大。这是因为随着信誉阈值的增大，可以筛选出信誉值高的边缘节点。节点的信誉值高意味着可靠性更高，使得区块链分片系统的效用更大。

结束语 本文提出了一种面向 6G 可信可靠智能的区块链分片与基于契约理论的激励机制，旨在为参与的每个边缘节点定制一组最优的契约，最大化区块链服务请求者的区块效用。作为能耗成本的补偿，最优的契约组合考虑节点的个性化隐私偏好，包括异构的计算能力和无线通信环境。为此，本文在信息完全对称和不完全对称的条件下求解出了一组最优契约，它们可以最大化区块链服务请求者的区块收益和可靠性需求，同时满足预算可行性、个体合理性和激励相容性约束。未来工作的一个方向是在区块链分片中加入跨片机制。

参 考 文 献

[1] GUO F, YU F R, ZHANG H, et al. Enabling massive IoT toward 6G: A comprehensive survey[J]. IEEE Internet of Things Journal, 2021, 8(15): 11891-11915.

[2] NGUYEN D C, DING M, PATHIRANA P N, et al. 6G Internet of Things: A comprehensive survey[J]. IEEE Internet of Things Journal, 2021, 9(1): 359-383.

[3] KHAYYAM H, JAVADI B, JALILI M, et al. Artificial intelligence and internet of things for autonomous vehicles[M]// Nonlinear Approaches in Engineering Applications. Cham: Springer, 2020: 39-68.

[4] KANG J, XIONG Z, JIANG C, et al. Scalable and communication-efficient decentralized federated edge learning with multi-blockchain framework[C]// International Conference on Blockchain and Trustworthy Systems. Singapore: Springer, 2020: 152-165.

[5] SUN W, LEI S, WANG L, et al. Adaptive federated learning and digital twin for industrial internet of things[J]. IEEE Transactions on Industrial Informatics, 2020, 17(8): 5605-5614.

[6] MOZUMDER M A I, SHEERAZ M M, ATHAR A, et al. Overview: Technology Roadmap of the Future Trend of Metaverse based on IoT, Blockchain, AI Technique, and Medical Domain Metaverse Activity[C]// 2022 24th International Conference on Advanced Communication Technology (ICACT). IEEE, 2022: 256-261.

[7] XIE J, ZHANG K, LU Y L, et al. Resource-efficient DAG Blockchain with Sharding for 6G Networks[J]. IEEE Network, 2021, 36(1): 189-196.

[8] FENG L, YANG Z, GUO S, et al. Two-layered blockchain architecture for federated learning over mobile edge network[J]. IEEE Network, 2021, 36(1): 45-51.

[9] HU S, LIANG Y C, XIONG Z, et al. Blockchain and artificial intelligence for dynamic resource sharing in 6G and beyond[J]. IEEE Wireless Communications, 2021, 28(4): 145-151.

[10] WANG W, JIAO Y, CHEN J, et al. Multi-Dimensional Contract Design for Blockchain Deployment in WSN under Information Asymmetry[C]// 2021 IEEE Globecom Workshops. IEEE, 2021: 1-6.

[11] YANG X Y, PENG C G, YANG H, et al. Rational PBFT Consensus Algorithm with Evolutionary Game[J]. Computer Science, 2022, 49(3): 360-370.

[12] JIAO Y, WANG P, NIYATO D, et al. Auction mechanisms in cloud/fog computing resource allocation for public blockchain networks[J]. IEEE Transactions on Parallel and Distributed Systems, 2019, 30(9): 1975-1989.

[13] LI J, LIU T, NIYATO D, et al. Contract-Theoretic Pricing for Security Deposits in Sharded Blockchain with Internet of Things (IoT)[J]. IEEE Internet of Things Journal, 2021, 8(12): 10052-10070.

[14] LI J, NIYATO D, HONG C S, et al. Cyber Insurance Design for Validator Rotation in Sharded Blockchain Networks: A Hierarchical Game-Based Approach[J]. IEEE Transactions on Network and Service Management, 2021, 18(3): 3092-3106.

[15] MANSHAEI M H, JADLIWALA M, MAITI A, et al. A game-theoretic analysis of shard-based permissionless blockchains[J]. IEEE Access, 2018, 6: 78100-78112.

[16] CHEN C, MA Q, CHEN X, et al. User Distributions in Shard-based Blockchain Network: Queueing Modeling, Game Analysis, and Protocol Design[C]// Proceedings of the Twenty-second International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing. 2021: 221-230.

[17] SUN W, LEI S, WANG L, et al. Adaptive federated learning and digital twin for industrial internet of things[J]. IEEE Transactions on Industrial Informatics, 2020, 17(8): 5605-5614.

[18] YUN J, GOH Y, CHUNG J M. DQN-based optimization framework for secure sharded blockchain systems[J]. IEEE Internet of Things Journal, 2020, 8(2): 708-722.

[19] ZHANG Y, SONG L, SAAD W, et al. Contract-based incentive mechanisms for device-to-device communications in cellular networks[J]. IEEE Journal on Selected Areas in Communications, 2015, 33(10): 2144-2155.

[20] SUN P, CHE H, WANG Z, et al. Pain-FL: Personalized privacy-preserving incentive for federated learning[J]. IEEE Journal on Selected Areas in Communications, 2021, 39(12): 3805-3820.

[21] GAO L, WANG X, XU Y, et al. Spectrum trading in cognitive radio networks: A contract-theoretic modeling approach[J]. IEEE Journal on Selected Areas in Communications, 2011, 29(4): 843-855.

WANG Si-ming, born in 1993, postgraduate. His main research interests include edge computing and blockchain.

YU Rong, born in 1979, Ph. D, professor, Ph.D supervisor. His main research interests include vehicular networks and blockchain.

（责任编辑：柯颖）