

信誉驱动的区块链分片共识及激励机制设计

田汉文^{1,2}, 张淑慧^{1,2}, 王连海^{1,2}, 徐淑奖^{1,2}, 邵蔚^{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系統安全重点实验室, 山东省基础科学研究中心 (计算机科学), 山东 济南 250014)

摘要: 当前, 实用性拜占庭容错 (PBFT, practical Byzantine fault tolerance) 共识算法在区块链分片环境下面临通信复杂度高、领导节点选举随机、共识节点不安全以及共识系统缺乏激励等问题。而信誉机制可以根据节点的行为和表现进行评估和奖惩, 提高系统对节点的信任度, 并促进节点的积极参与和诚实行为。基于此, 提出了信誉驱动的区块链分片共识及激励机制。在基于信誉管理的分片系统中, 采用聚合签名技术将多个共识节点的签名合并为一个, 通过信誉评估确定节点的投票权重, 大大减少了通信开销并提高了共识的平等性和安全性; 同时, 在信誉管理下提出一种押金与激励机制, 当节点初入网络时设置最低门票标准, 并根据信誉值随时间逐步增加, 根据节点的角色和分工的不同, 采用基础奖励与有效奖励结合的激励模式, 从而有效平衡节点的稳定收益和动态奖励, 不断提升网络的稳定性和安全性。实验结果显示, 所提共识算法R-PBFT相比PBFT, 具有较小的时延和较高的吞吐量, 有效地提高了系统性能; 与单纯按照信誉等比分配的激励机制相比, 所提激励机制具有更高的共识参与率。

关键词: 区块链; 分片技术; 信誉; 实用拜占庭容错 (PBFT) 共识算法; 激励

中图分类号: TP393

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2025002

Design of reputation-driven blockchain sharding consensus and incentive mechanism

TIAN Hanwen^{1,2}, ZHANG Shuhui^{1,2}, WANG Lianhai^{1,2}, XU Shujia^{1,2}, SHAO Wei^{1,2}

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

收稿日期: 2024-03-28; 修回日期: 2024-08-09

通信作者: 张淑慧, zhangshh@sdas.org

基金项目: 泰山学者计划 (tsqn202312231); 国家自然科学基金 (62102209); 山东省自然科学基金 (ZR2024MF104); 山东省重点研发计划项目 (2021CXGC010107); 济南市“新高校20条”资助项目 (202228017)

Foundation Items: Taishan Scholars Program (tsqn202312231), The National Natural Science Foundation of China (62102209), The Natural Science Foundation of Shandong Provincial (ZR2024MF104), Shandong Provincial Key Research and Development Program (2021CXGC010107), The New 20 Project of Higher Education of Jinan, China (202228017)

引用格式: 田汉文, 张淑慧, 王连海, 等. 信誉驱动的区块链分片共识及激励机制设计[J]. 网络与信息安全学报, 2025, 11(1): 141-150.

Citation Format: TIAN H W, ZHANG S H, WANG L H, et al. Design of reputation-driven blockchain sharding consensus and incentive mechanism[J]. Chinese Journal of Network and Information Security, 2025, 11(1): 141-150.

Abstract: The PBFT (Practical Byzantine Fault Tolerance) consensus algorithm was confronted with several challenges in the blockchain sharding environment, including high communication complexity, random leader election, node insecurity, and insufficient participation incentives. To address these issues, a reputation-driven blockchain sharding consensus and incentive mechanism was proposed. Reputation mechanisms were utilized to evaluate and incentivize node behavior, thereby enhancing system trust and promoting active participation. Aggregated signature technology was employed to merge consensus node signatures, and node voting weights were determined based on reputation assessments, which reduced communication overhead and improved consensus equality and security. Additionally, a deposit and incentive mechanism was introduced under reputation management, where initial entry standards were set and gradually increased over time according to reputation values. Differentiated incentive models, based on node roles, were designed to balance stable income and dynamic rewards, thereby continuously improving network stability and security. Simulation results demonstrated that the proposed R-PBFT consensus algorithm outperformed the traditional PBFT, maintaining lower latency and higher throughput, which effectively enhanced system performance. Furthermore, compared to proportional incentive allocation based solely on reputation, the proposed incentive mechanism achieves higher consensus participation rates.

Keywords: blockchain, sharding technique, reputation, PBFT consensus algorithm, incentive

0 引言

区块链作为分布式账本的重要技术之一,已广泛应用于供应链、政府治理、金融和游戏等领域^[1-4]。但是,区块链中的节点需验证和存储所有交易带来了低吞吐量和高时延问题,面临着严重的可扩展性挑战^[5-6]。分片技术作为一种链上扩容技术,能够将区块链网络划分为多个分片,由各自的节点处理事务和存储状态,解决了区块链的可拓展性问题,且在不影响中心化程度的同时提升了性能,已成为区块链主流的扩容方法之一^[7]。

在区块链分片中,共识机制确保了分片网络中节点的一致性和可信度,实现了交易有效性和数据同步的共识。实用性拜占庭容错(PBFT, practical Byzantine fault tolerance)^[8]共识算法是一种经典的共识算法,将其应用在分片内部的共识过程中,可以在保持容错性的同时提高交易吞吐量。然而,PBFT算法采用多轮通信和投票机制,通信复杂度高,且缺乏惩罚机制,影响了系统的可靠性和安全性。

在基于信誉的分片系统中,信誉评估为节点选择、系统的安全性和共识机制提供了重要保障^[9]。通过信誉评估,可以选出一部分具有较高信誉值的节点参与共识过程,或者由选举出的领导节点主导PBFT共识,以降低系统开销。然而,这种方法可能会引入一定程度的中心化风险。当攻击者集中攻击领导节点时,整个共识过程可能会

中断。此外,上述区块链分片共识机制并不能确切地识别出恶意节点。当恶意节点拥有与正常节点相同的投票权时,它们有可能联合起来破坏系统的安全性^[10]。同时,在基于信誉的分片系统中,押金和激励机制的研究尚未充分展开。押金和激励机制旨在激励节点遵守协议规则,维护网络的安全和稳定运行。然而,在实际的区块链系统中,由于节点之间的计算能力和验证交易的效率不同,平均分配奖励可能无法有效激励节点诚实地执行工作,同时也可能影响系统激励的公平性。

针对上述PBFT共识算法通信复杂度高、节点缺乏积极性等问题,本文利用信誉管理对节点进行奖惩评估,并结合领导者选举机制,提出了一种信誉驱动的区块链分片共识算法。该算法在信誉管理的基础上赋予节点不同的影响力,并为节点的激励机制提供依据,以确保共识机制的可靠性和安全性。

本文的主要贡献如下。

1) 提出一种基于信誉的区块链共识算法R-PBFT,通过采用聚合签名技术,将多个节点的签名合并成一个,通过信誉评估确定节点的投票权重,从而降低通信成本,增强共识的公平性和安全性。

2) 在信誉机制下引入了押金和激励机制,当节点初入网络时,需满足最低门槛(缴纳系统设置的最低押金金额),并根据信誉值随时间逐步增加押金;同时,根据节点角色设定不同的奖励模式,平衡稳定收益与动态激励,有助于提升网

络的稳定性和安全性。

3) 对 R-PBFT 进行了共识时延、吞吐量等性能测试, 并对所提出的激励机制进行测试。实验表明, 本文所提方案能够有效解决 PBFT 的通信复杂度高、节点缺乏积极性问题。

1 研究现状

PBFT 共识算法是一种基于拜占庭容错理论的分布式共识算法^[11], 旨在解决分布式系统中可能出现的拜占庭故障。在 PBFT 共识算法中, 网络中的节点按照一定的规则被选举为领导节点, 领导节点负责提出区块和执行交易的顺序。假如节点总数为 n , 故障节点数为 f , 当 $n > 3f$ 时才能达成拜占庭协定。然而在 PBFT 的通信过程中, 准备与确认过程时间复杂度达到 $O(n^2)$, 在实际应用中具有较高的计算和通信开销。其次, PBFT 共识算法在领导节点的选择方面存在一些随意性, 因为领导节点是按顺序选择的, 而且所有节点都被视为共识节点, 这可能会影响领导节点的可靠性和节点的积极性。此外, PBFT 共识算法对共识节点缺乏奖惩措施, 即使存在拜占庭节点, 也没有相应的惩罚机制, 可能会影响系统的安全性。

近年来, 许多学者针对 PBFT 共识算法的不足进行了改进。DBFT^[12]将 PBFT 与委托权益证明 (DPoS, delegated proof of stake)^[13] 算法相结合, 其中共识节点由 DPoS 算法中的股份投票方式选举产生, 以降低通信过程的复杂性, 优化 PBFT 的共识流程。Fu 等^[14]采用了聚合签名的方式, 领导者可以通过收集节点的签名来生成一个总的门限签名, 从而减少通信量。在基于信誉的分片系统中, 信誉评估有助于选出行为可靠的节点并识别和排除恶意节点, 为共识机制提供了重要的参考依据^[15]。因此常有一些解决方案依据信誉值选出部分“优异”的节点参与共识, 或者由选举出的领导节点来主导 PBFT 共识, 以达到降低系统开销的目的。GR-PBFT^[16]引入了信誉奖惩机制来改进领导节点的选举方式, 以提高领导节点的可靠性。在这种机制下, 共识确认阶段由领导节点负责消息对比, 避免了消息之间的两两交互, 总体通信开销有所减少。但是, GR-PBFT 的通信复杂度仍然是 $O(n^2)$ 。T-PBFT^[17]采用了 EigenTrust 模型, 通过对节点行为的评估来确定其信任可靠

性, 并选出系统中质量较高的节点构建新的共识小组, 从而降低系统通信的复杂度。然而, 这样很可能引入某种程度的中心化风险, 当攻击者集中攻击领导节点时, 整个共识过程将会中断。

在共识激励机制的研究方面, Yang 等^[18]指出有共识算法中缺少激励机制等问题。Man-shaei 等^[19]针对区块链分片的共识协议设计了激励机制, 这些激励措施有助于促进分片内部的合作并防止合谋攻击。Chen 等^[20]研究了如何在基于分片的区块链中正确分配用户, 以提升系统的交易性能。Zhou 等^[21]针对懒惰或低信誉节点问题, 实行奖惩机制, 即对共识中诚信表现的节点予以奖励, 并对错误行为的节点实施惩罚。然而, 在实际的区块链系统中, 各个节点的计算能力存在差异以及在验证交易过程中的表现各不相同, 若采取均分奖励方式, 将无法有效激励节点保持诚实的工作状态。

综上所述, 在分片共识机制的改进上, 研究者针对 PBFT 的通信复杂度以及激励机制问题进行了多方面的改进。信誉的引进为共识节点的选举提供了重要的安全保障。然而, 如果只选举部分节点进行共识, 就会产生中心化的风险; 而且, 当恶意节点拥有和正常节点同样的投票权时, 恶意节点很有可能联合起来破坏系统的安全性。同时, 在基于信誉的分片系统中, 缺少对押金和激励机制的研究。押金和激励机制可以激励节点遵守协议规则, 保护整个网络安全和稳定运行。因此, 继续研究基于信誉驱动的区块链分片共识以及激励机制是非常有必要的。

2 基于信誉的区块链分片共识方法

2.1 方案概述

本文基于文献[22]中监管委员会与普通分片协作的分片系统进行共识算法的改进。考虑到 PBFT 共识算法本身对恶意节点没有专门的惩罚机制, 文献[22]引入了信誉管理机制对节点的行为进行奖惩评估, 对低于阈值的节点进行淘汰处理。根据节点累积的信誉, 在每个分片内随机选择领导节点和备选领导节点, 有助于确保 PBFT 共识过程的可靠性和安全性, 可以有效防止拜占庭行为和恶意攻击, 从而维护整个系统的稳定运行和可信度。在此信誉管理分片架构的基础上,

本文提出的信誉驱动的区块链分片共识及激励机制总体框架如图 1 所示。

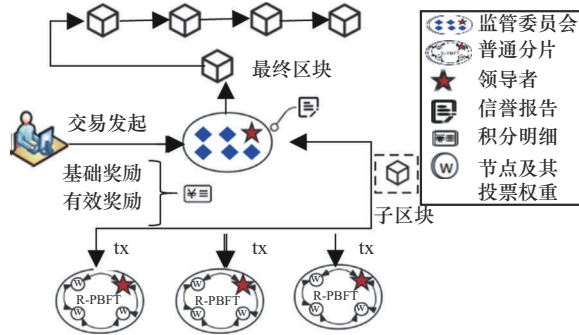


图 1 信誉驱动的区块链分片共识及激励机制总体框架

Figure 1 Overall framework of reputation-driven blockchain sharding consensus and incentive mechanism

在每个 PBFT 共识轮中, 使用 BLS (Boneh-Lynn-Shacham) 聚合签名算法对所有节点的签名进行聚合, 设置节点的投票权重与其信誉成正比, 以保证在预备和提交阶段正确利用备份节点的投票权重, 从而实现分布式一致性。此外, 在押金的经济基础上设置不同角色差异化的激励制度。本文方案的核心为 R-PBFT 共识算法和押金激励机制。

1) R-PBFT 共识算法。采用聚合签名技术将多个节点的签名合并成一个, 从而减少共识过程的通信开销。同时, 根据节点的信誉分数来确定节点的投票权重, 能够更可靠地衡量节点的可信度和贡献度。

2) 押金激励机制。当节点加入区块链分片系统时, 需要向网络的共有账户支付一定数额的押金。同时, 根据节点角色分工的不同, 分为领导节点和普通备份节点, 各自采用基础奖励与有效奖励结合的激励模式。

2.2 信誉管理

(1) 信誉计算

监管委员会在收到分片领导者发来的子区块 (其中包含领导本身的签名、所有验证节点的签名以及验证交易时的反应时间) 后, 对比交易处理结果。监管委员会基于验证者的行为以及性能特征, 通过信誉评价计算出本轮节点的信誉分数。通过式 (1) 可以求出节点信誉值的影响因子 δ_i 。

$$\delta_i = \begin{cases} 0 \\ \rho \times \delta_{i-1} + (1 - \rho) \times \left(\sum_{j=1}^l S(j) \times \alpha_j \times C \right) \end{cases} \quad (1)$$

其中 δ_{i-1} 为节点的历史因子, l 为验证交易的数量, $S(j)$ 为奖励或者惩罚系数, C 为节点初始分配的性能等级。 α_j 为验证结果系数, 对比交易结果, 当节点验证结果正确时取值为 1, 错误时取值为 -1。 ρ 为时间衰减因子, 用来调节历史信誉的有效性。 ρ 的取值范围为 (0,1)。 ρ 值越大, 代表更看重验证节点过往的分数累积; 相反, 则是更看重本周期的计算分数。

(2) 节点淘汰

在计算完所有验证节点的信誉值后, 对于分数未达到阈值的节点, 由监管委员会中的所有负责人分别对此节点发出投票交易后进行淘汰处理。其中阈值可以在不同网络环境中具体设置。

领导节点将驱逐结果进行广播, 删除被驱逐节点的地址并丢弃它的公钥。所有节点更新网络视图, 监管委员会对系统的信誉列表进行更新。如果一个被驱逐的节点重新加入网络, 那么它必须重新加入一个新的密钥对, 并且将丢弃过往所有的分数积累。这样有助于激励节点的诚实行为。

(3) 领导者选举

在分片形成后, 在各分片选举信誉分数位于前 50% 的节点作为领导者区间, 并在区间内随机选择出分片的领导者和备选领导者。备选领导者需要监督领导者的行为。在共识过程中, 当恶意领导者出现罢工、扣留消息等行为时, 分片中的诚实节点如果无法在响应时间内接收到领导者的消息, 就会向分片中的其他节点广播紧急通知, 由备选领导者上报监管委员会并进行备选替补。特别说明的是, 上一轮是领导者的节点本轮不出现在选择区间内。

2.3 R-PBFT 共识算法

在信誉驱动的区块链分片共识方法中, 假设要签署的消息为 m , G 为曲线上的一个生成点。对于一个节点 i , 随机生成私钥 sk_i , 并通过椭圆曲线点乘运算得到公钥 pk_i 。 $pk_i = sk_i \times G$, 即私钥 sk_i 乘以基点 G 得到公钥 pk_i 。

设置节点 i 的投票权重 W_i 与其信誉分数 R_i 成正

比, 由 $W_i = R_i \times k$ 可以计算出投票权。其中 k 是一个调整系数, 在实际应用中用于控制信誉分数与投票权之间的线性关系。较大的 k 值将导致较大的差异, 而较小的 k 值将减小差异。在本文中, 为了减小差异以及方便计算, k 设置为 0.2。

R-PBFT 算法共识过程如图 2 所示, 包括请求 (request)、预准备 (pre-prepare)、准备 (prepare)、提交 (commit) 和响应 (reply) 5 个阶段。

1) 请求阶段。当交易进入分片时, 客户端向领导节点发送请求 $\langle \text{request}, o, t, c_{\text{sig}} \rangle$, 其中 o 为客户端请求的操作, t 为时间戳, c_{sig} 表示客户端 c 对请求消息的签名。领导节点接收客户端发送的请求消息并将其写入日志, 此时交易进入分片。

2) 预准备阶段。领导节点广播预准备消息给所有分片内参与共识的备份节点。消息的内容为 $\langle \text{pre-prepare}, v, n, d \rangle, l_{\text{sig}}, m \rangle$, 其中 v 为试图编号, n 为序列号, d 为消息 m 的摘要, l_{sig} 为领导节点的签名。

3) 准备阶段。备份节点 i 在收到领导节点发送的交易消息 m 后, 对该消息进行校验, 校验无误后向领导节点发送准备消息并附上签名以及自己的投票权重。消息的内容为 $\langle \text{prepare}, v, n, d, w_i, s \rangle$, 其中 w_i 为节点的投票权重, s 为该普通备份节点的签名。使用私钥 sk_i 对消息 m 进行签名, 根据 $\text{sig}_i = sk_i \times H(m)$ 计算生成个体签名 sig_i , 其中 $H(m)$ 是消息的哈希值。分片内 n 个节点的签名集表示为 $S = \{ \text{sig}_1, \text{sig}_2, \dots, \text{sig}_n \}$ 。

当领导节点收到一条准备消息时, 校验成功

后将其写入日志。当领导节点已收到请求 m 以及收到 $2f$ 条对应的来自不同备份节点的准备消息后, 计算收到的准备消息中的权重总和, 以确定超过 $2/3$ 的总权重。领导节点聚合所有签名 sig_i , 合并为一条消息, 广播给所有的备份节点。备份节点收到消息并成功验证后进入提交阶段。

4) 提交阶段。节点 i 向领导节点发送提交消息 $\langle \text{commit}, v, n, d, w_i, s \rangle$, 当领导节点收到一条提交消息时, 校验成功后将其写入日志。当请求 m 已经准备好并且领导节点已经收到 $2f+1$ 条对应的来自不同节点 (可包括自己) 的提交消息, 确定已经达到 $2/3$ 的权重后, 聚合所有签名 sig_i , 合并成一条消息, 广播给所有的备份节点。

5) 响应阶段。系统中每个分片内的节点将执行结果响应至客户端。

在共识的各阶段中, 通信总量为 $1 + (n-1) + 2(n-1) + 2(n-1) + n = 5n - 4$ 条消息, 使得网络的通信量从原始 PBFT 的 $O(n^2)$ 降低至 $O(n)$, 大大减少了共识过程的通信开销。

2.4 系统押金设置

当一个节点想要加入区块链系统时, 首先需要向系统的共有账户缴纳一定数额的押金。在分片系统中设置一个最低押金标准, 以防止信誉分数过低的节点加入。对于缴付的押金, 依据节点的信誉分数, 表现良好的节点可以获得押金的退还以及相关激励, 而不良行为的节点在信誉分数低于阈值时会被驱逐出网络并扣除押金。

此外, 为鼓励节点保持高标准的行为, 使用

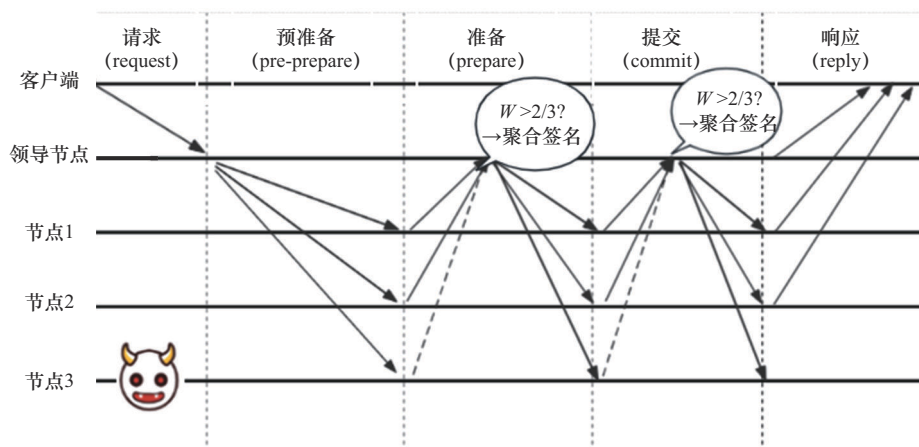


图2 R-PBFT算法共识过程

Figure2 Consensus process of R-PBFT algorithm

逐步增加的押金机制。节点在初始加入网络时需要缴纳较低的押金,随着时间的推移,根据节点的表现(即信誉值),押金将逐步增加。在周期 t 中,由 $D_t = D_{t-1} \times \sigma / R_i$ 可以计算出押金 D_t ,表示为上一周期押金和节点信誉分数负相关的加和,其中 R_i 为节点的信誉分数, σ 为调节系数。为确保节点在网络中稳定运行,节点在完成一轮工作后并不能立刻退还,而是需要在网络中锁定一段时间,避免恶意节点多次加入退出网络,从而影响系统效率。

2.5 激励机制

在区块链分片架构的激励机制设置中,本文将节点信誉分数纳入奖励分配的考量因素,采用基础奖励+有效奖励的模式,并根据节点的分工不同,设计不同的计算方式。

所谓“基础奖励”,是为鼓励节点能积极参与网络,保障每个节点都可以获得一定的基础奖励。将所有交易费 f 拿出 α 百分比作为基础奖励,均分给所有的节点(前提是在一个周期评分后没有被淘汰的节点)。即在一个节点数量为 n 的分片中,每个节点分得的基础奖励为 $\frac{\alpha f}{n}$ 。

所谓“有效奖励”,针对节点的分工不同有不同的计算规则。对于备份节点,通过计算节点在所属分片的信誉分数占比,从剩余的交易费即 $(1 - \alpha)f$ 中分得有效奖励;对于分片内的领导节点,则根据其所负责的打包子区块的效率获得相应的区块奖励作为有效奖励。

利用式(2)可以求出备份节点在其所属分片的信誉分数占比。

$$P_i = \frac{R_i}{\sum_{j=1}^n R_j - R_{i=L}} \quad (2)$$

其中, R_i 为一个周期后节点 i 计算得出的信誉分数, n 为节点所属分片中节点的数量, L 为所属分片中的领导节点, $R_{i=L}$ 为该分片中领导节点的信誉分数。

因此,备份节点最后获得的激励为

$$I_i = (1 - \alpha)f \times P_i + \frac{\alpha f}{n} \quad (3)$$

对于领导节点的有效奖励,考虑到其工作过程需要收集备份节点的签名,为了减少领导节点受利益驱使而恶意漏掉普通节点签名的行为,将

领导节点打包进子区块的签名数量占比作为区块奖励的评分标准,假设区块奖励表示为 R_{block} ,则领导节点的有效奖励占比为

$$P_{i=L} = \frac{\text{Sig}}{\sum_{i=1}^s \text{sig}_i} \quad (4)$$

其中, Sig 为此分片中领导节点打包进子区块的普通备份节点的签名数量, sig_i 为共识过程中领导节点收集的备份节点 i 的签名, s 为共识过程中可以收集的备份节点数量。 $P_{i=L}$ 表示领导节点打包进子区块的签名数量与收集的签名数量的比值。

因此领导节点最后获得的激励为

$$I_{i=L} = R_{\text{block}} \times P_{i=L} + \frac{\alpha f}{n} \quad (5)$$

本文的激励机制采用了基础奖励和有效奖励组合方式。领导节点通过负责打包子区块的效率来获得相应的区块奖励,而备份节点根据其在分片中的信誉分数占比获得有效奖励。备份节点和领导节点的激励来源有所不同,使得领导节点与备份节点之间没有绝对的竞争关系。这样可以避免恶意领导节点故意漏掉一些节点的签名与其他节点合谋作恶,提升了网络的稳定性和安全性。

这种押金和激励机制不仅能够增强网络的安全性和信任度,还能够激励节点的良好行为、降低恶意攻击风险,从而促进区块链分片网络的健康运行和发展。

3 仿真实验及分析

本实验基于 Python 编程语言对本文提出的算法进行仿真测试。实验在配置为 64 GB 内存、i7-10700 处理器和 Ubuntu 20.04 操作系统的计算机上进行。实验着眼于比较 PBFT 算法和 R-PBFT 算法在共识时延和吞吐量方面的性能表现。为验证 R-PBFT 共识算法的有效性,本文进行了 BLS 聚合签名时延的测试;同时,通过对共识参与率的测试和评估,深入探讨了激励机制在共识过程中的作用。这些比较和评估将有助于更全面地理解和优化分布式共识算法的性能和可靠性。

3.1 共识时延测试

在区块链系统中,共识时延指完成一轮共识所需的时间,通常由几个方面的时延组成。首先是消息传输的时延,即消息从一个节点传输到另

一个节点所需的时间，这取决于网络拓扑、带宽等因素。其次是节点处理的时延，即节点收到消息后处理和验证消息的时间。最后是共识算法本身的时延，即共识算法执行的时间，包括投票、验证和达成共识的时间。

在PBFT共识算法中，时延主要集中在几个阶段。在预准备消息、准备消息和提交消息阶段，节点都需要等待收集到足够多的消息，这些等待时间会影响PBFT共识的整体时延。在本文提出的R-PBFT共识算法中，共识时延主要受到PBFT算法的基础时延和引入的聚合签名、信誉投票权重计算的影响。实验中设置节点数量从5增加到40个，进行20次测试并取共识时延的平均值。PBFT与R-PBFT共识算法的共识时延结果对比如图3所示。

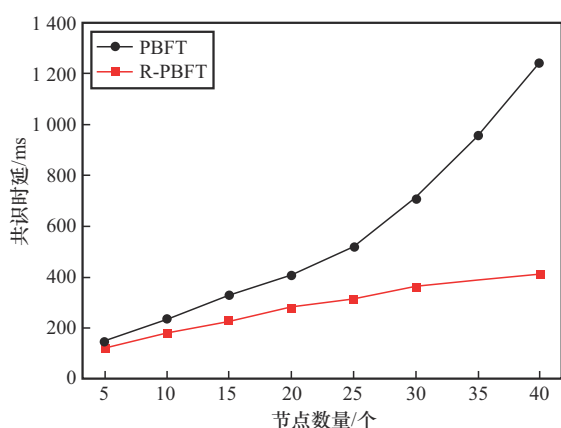


图3 共识时延结果对比

Figure 3 Comparison of consensus delay results

由实验结果可以看出，随着节点数量的增加，PBFT和R-PBFT的共识时延都逐渐增大；在不同的节点数量下，R-PBFT算法的共识时延都低于PBFT算法。这是因为在PBFT共识过程中，每个备份节点都必须与其他节点进行通信——通信复杂度为 $O(n^2)$ ，随着分区内节点数量的增加，节点之间的通信量迅速增加，从而导致共识时延快速增长。而R-PBFT算法引入了聚合签名，并设置节点依据其信誉值有不同的投票权重，使得算法的复杂度降至 $O(n)$ 。从实验结果来看，R-PBFT的共识时延远小于PBFT，表明R-PBFT算法在共识过程中具有更高的效率和更快的速度，能够更快地达成共识并确认交易的有效性。

3.2 吞吐量测试

吞吐量 (TPS, transactions per second) 指在单位时间内系统处理的交易数量。吞吐量作为评估共识算法效率的标准，体现了系统处理交易的速度和效率。更高的吞吐量意味着系统能够更快速地处理更多的交易，从而更好地满足用户需求。因此，吞吐量的增加通常被视为共识算法性能优化的重要指标。由式(6)可以计算出TPS，其中transaction为 Δt 时间内打包进区块的交易总数， Δt 为出块时间。

$$TPS = \frac{\text{transaction}}{\Delta t} \quad (6)$$

实验中设置节点数量由5增加到40，使用客户端发送了1000次交易请求，以测试两种算法的吞吐量。为了确保实验结果的一致性和可靠性，提取20次实验数据的平均值进行分析。PBFT、R-PBFT共识算法的吞吐量测试结果对比如图4所示。

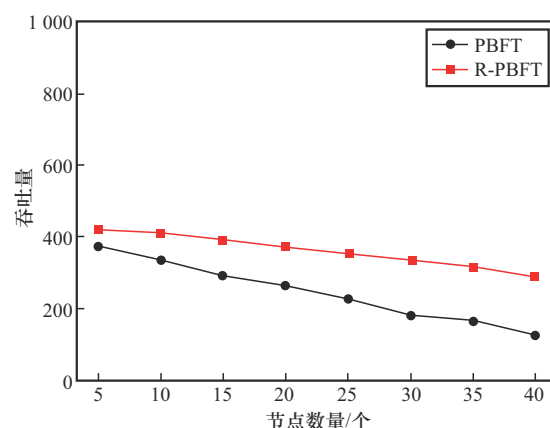


图4 吞吐量测试结果对比

Figure 4 Comparison of throughput test results

由实验结果可知，随着节点数量的增加，两种共识算法的吞吐量都呈下降趋势，但R-PBFT的吞吐量性能更优异。这是因为R-PBFT中的通信量较小，随着节点数量的增加，R-PBFT共识算法能有效减少领导节点的恶意行为，降低因节点动态变化引起的资源开销，从而使得其吞吐量的下降趋势与PBFT共识算法相比更为稳定。

3.3 聚合签名时延

本文提出的R-PBFT算法使用了BLS聚合签名，因此在测试中需要分析聚合签名的生成时间和验证时间，以确定其是否会对整个共识过程的

性能产生影响。这里的聚合签名时延指从聚合开始到合并一个聚合签名所需的时间，而验证聚合签名时延则是从验证开始到验证完成所需的时间。

在本节实验中，分别模拟了分片内有 50、100、150、200、250、300、350、400 个签名进行聚合，每个签名使用不同的公私钥进行签署，并对聚合签名函数进行了性能测试。同样，测试中使用了对应于 50、100、150、200、250、300、350、400 个签名的公钥组对聚合后的签名进行验证，以确定验证聚合签名的成本。聚合签名以及验证聚合签名的时延如图 5 所示。

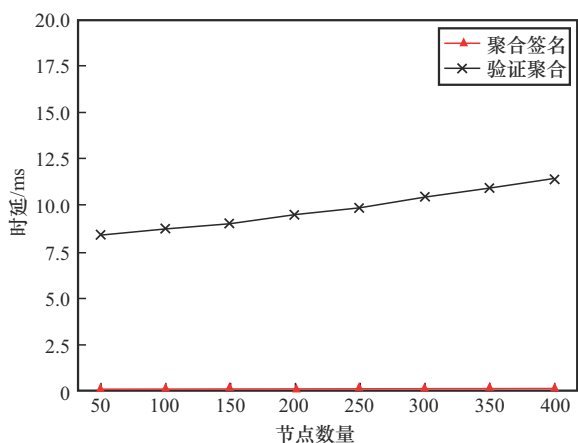


图5 聚合签名以及验证聚合签名的时延

Figure 5 Aggregation signature and the latency of verifying the aggregation signature

从实验结果可以看出，验证一个由多个签名聚合而成的聚合签名所需的时间比聚合多个签名所需的时间稍多，但并不足以影响整个网络的性能。验证一个由 400 个签名聚合而成的聚合签名仅需要 11.4 ms。因此，相较于第 3.1 节测得的共识总时延，将聚合签名与 PBFT 共识算法相结合不但不会显著增加网络开销，还能够有效改善 PBFT 算法中全广播通信的高开销问题，解决了 PBFT 算法在节点增加时性能急剧下降的问题，有助于提升整个网络的可扩展性。

3.4 共识参与率测试

激励机制能够促使节点更加积极地参与共识，因为它提供了经济或其他方面的奖励，从而增加了节点参与共识的动力。共识参与率是区块链网络中节点参与共识的程度衡量标准。它反映

了网络中节点对于确认交易和验证区块的积极性和频率。高参与度意味着更多的节点参与到共识过程中，从而增强了网络的安全性和去中心化程度。在本节实验中，设置每个分片 250 个节点，运行 10 个周期，对比本文方案的激励机制和单纯按照信誉等比分配的激励机制，节点共识参与率测试结果如图 6 所示。

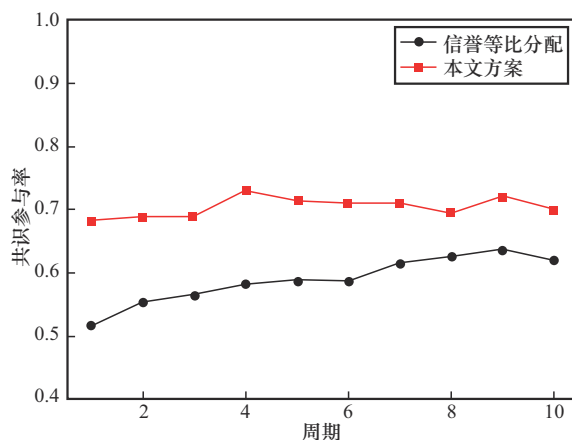


图6 节点共识参与率测试结果

Figure 6 Node consensus participation rate test results

由实验结果可以看出，本文方案的激励机制比单纯按照信誉等比分配的激励机制有更高的共识参与率。在信誉的基础上采取基础激励和有效激励组合方式，可以确保即使是信誉较低的节点也能够获得一定的激励，从而促进低分数节点的积极参与。本文方案基于分工的激励制度，避免了单纯按照信誉等比分配激励可能带来的竞争和焦虑问题，使节点更加专注于完成自己的任务，而不是过分关注信誉得分。这样可以避免恶意领导节点故意漏掉一些节点的签名与其他节点合谋作恶，提升了网络的稳定性和安全性。这说明本文基于信誉设置不同分工的激励制度并为每个节点存留基础的激励，可以更好地激励节点参与共识，提高整个分片网络的韧性和稳定性。

3.5 功能对比与分析

本文所提算法与 PBFT 以及 GR-PBFT 共识算法的比较如表 1 所示。

本文所提 R-PBFT 算法和 GR-PBFT 都基于信誉管理对 PBFT 进行改进。在 GR-PBFT 算法中，根据节点信誉分数选举领导节点，在共识的确认阶段由领导节点进行消息的对比，而不再需要两

两交互消息。这样虽然可以减少通信开销，但是总体的通信复杂度还是 $O(n^2)$ 。而本文所提算法，基于信誉管理引入了聚合签名，将共识的通信复杂度降低至 $O(n)$ ；此外，根据节点的信誉评分确定其投票权重，从而提升了共识的安全性。为了更好地激励节点积极参与共识，本文还在激励机制方面进行了研究，根据节点的不同角色设置了基础奖励和有效奖励相结合的激励机制。

表1 共识算法比较

Table 1 Comparison of consensus algorithms

算法	基于信誉	节点投票权重	激励	通信复杂度
PBFT ^[8]	×	×	×	$O(n^2)$
GR-PBFT ^[16]	√	×	—	$O(n^2)$
本文算法	√	√	√	$O(n)$

4 结束语

本文对 PBFT 算法中存在的通信复杂度高、领导节点选举随机、共识节点不安全以及共识系统缺乏激励等问题进行了研究，提出了信誉驱动的区块链分片共识及激励机制。在基于信誉的分片系统中，充分利用信誉管理对节点的奖惩评估以及领导者选举机制，并采用聚合签名技术将多个共识节点的签名融合为一个，通过信誉评估确定节点的投票权重，从而减少了通信开销，提升了共识的公平性和安全性。同时，引入了押金和激励机制，通过逐步增加押金，来鼓励节点保持高水平行为，即信誉分数越高，其押金增长越慢；针对不同节点角色采用基础奖励与有效奖励相结合的激励方式，有效平衡了节点的稳定收益与动态激励，有助于不断提升网络的稳定性和安全性。实验结果表明，本文提出的 R-PBFT 共识算法在性能上能够保持较小的时延和较高的吞吐量，且有更高的共识参与率。在未来的工作中，将进一步研究信誉驱动的分片共识在不同场景下的适用性，提升系统的可扩展性和容错性，以适应不断增长的区块链网络需求。

参考文献：

[1] AN J, YANG H, GUI X, et al. TCNS: node selection with privacy protection in crowdsensing based on twice consensus of blockchain

[J]. IEEE Transactions on Network and Service Management, 2019, 16(3): 1255-1267.

[2] ZHANG M, ELIASSEN F, TAHERKORD A, et al. Demand-response games for peer-to-peer energy trading with the hyperledger blockchain[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2021, 52(1): 19-31.

[3] 张娴, 朱建明, 隋智源, 等. 数字货币交易匿名性与监管的博弈分析[J]. 网络与信息安全学报, 2022, 8(5): 150-157.

ZHANG X, ZHUN J M, SUI Z Y, et al. Analysis on anonymity and regulation of digital currency transactions based on game theory[J]. Chinese Journal of Network and Information Security, 2022, 8(5): 150-157.

[4] FERRAG M A, SHU L, CHOO K K R. Fighting COVID-19 and future pandemics with the internet of things: security and privacy perspectives[J]. IEEE/CAA Journal of Automatica Sinica, 2021, 8(9): 1477-1499.

[5] BEZ M, FORNARI G, VARDANEGA T. The scalability challenge of ethereum: an initial quantitative analysis[C]// Proceedings of 2019 IEEE International Conference on Service-Oriented System Engineering (SOSE). Piscataway: IEEE Press, 2019: 167-176.

[6] QI X, ZHANG Z, JIN C, et al. BFT-Store: storage partition for permissioned blockchain via erasure coding[C]// Proceedings of 2020 IEEE 36th International Conference on Data Engineering (ICDE). Piscataway: IEEE Press, 2020: 1926-1929.

[7] JIA D, XIN J, WANG Z, et al. Optimized data storage method for sharding-based blockchain[J]. IEEE Access, 2021, 9: 67890-67900.

[8] CASTRO M, LISKOV B. Practical byzantine fault tolerance[C]// Proceedings of the 3th Symposium on Operating Systems Design and Implementation (OSDI). Berkeley: USENIX Association, 1999: 173-186.

[9] 唐宏, 刘双, 酒英豪, 等. 实用拜占庭容错算法的改进研究[J]. 计算机工程与应用, 2022, 58(9): 144-150.

TANG H, LIU S, JIU Y H, et al. Improved study of practical Byzantine fault-tolerant algorithm[J]. Computer Engineering and Applications, 2022, 58(9): 144-150.

[10] 王梦楠, 黄建华, 邵兴辉, 等. 基于信誉的区块链分片共识方案[J]. 计算机科学, 2022, 49(10): 297-309.

WANG M N, HUANG S H, SHAO X H, et al. Reputation-based Blockchain Sharding Consensus Scheme[J]. Computer Science, 2022, 49(10): 297-309.

[11] LAMPORT L, SHOSTAK R, PEASE M. The Byzantine generals problem[M]. LAMPORT. Concurrency, 2019: 203-226.

[12] CRAIN T, GRAMOLI V, LARREA M, et al. DBFT: efficient leaderless byzantine consensus and its application to blockchains[C]// Proceedings of 2018 IEEE 17th International Symposium on Network Computing and Applications (NCA). Piscataway: IEEE Press, 2018: 1-8.

- [13] LARIMER D. DoPS consensus algorithm-the missing white paper[J]. Bit Share Whitepaper, 2017.
- [14] FU J H, ZHOU W H, XU M X, et al. New public blockchain protocol based on sharding and aggregate signatures[J]. Journal of High Speed Networks, 2021, 27(1): 83-99.
- [15] TONG W, DONG X W, ZHENG J W. Trust-PBFT: a peer trust-based practical byzantine consensus algorithm[C]// Proceedings of 2019 International Conference on Networking and Network Applications (NaNA). Piscataway: IEEE Press, 2019: 344-349.
- [16] 陈苏明, 王冰, 陈玉全, 等. 基于节点分组信誉模型的改进 PBFT 共识算法[J]. 计算机应用研究, 2023, 40(10): 2916-2921.
- CHEN S M, WANG B, CHEN Y Q, et al. Improved PBFT consensus algorithm based on node grouping reputation model[J]. Application Research of Computers, 2023, 40(10): 2916-2921.
- [17] GAO S, YU T, ZHU J, et al. T-PBFT: an eigentrust-based practical Byzantine fault tolerance consensus algorithm[J]. China Communications, 2019, 16(12): 111-123.
- [18] 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.
- [19] 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.
- [20] 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.
- [21] 周健, 张杰, 闫石, 等. 基于动态信任的区块链激励共识机制研究[J]. 计算机应用研究, 2021, 38(11): 3231-3235+3248.
- ZHOU J, ZHANG J, YAN S, et al. Study on consensus mechanism of blockchain motivation based on dynamic trust[J]. Application Research of Computers, 2021, 38(11): 3231-3235+3248.
- [22] ZHANG S, TIAN H, WANG L, et al. A reputation-based dynamic reorganization scheme for blockchain network sharding[J]. Connection Science, 2024, 36(1): 2327438.

[作者简介]



田汉文 (1998-), 女, 山东临沂人, 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。



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。



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。



邵蔚 (1994-), 女, 山东济南人, 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, 主要研究方向为区块链、隐私保护。