计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.210900110

基于演化博弈的理性拜占庭容错共识算法

杨昕宇[1,3]　彭长根[1,2,3]　杨　辉[1]　丁红发[4]
1 贵州大学数学与统计学院公共大数据国家重点实验室　贵阳 550025
2 贵州大学计算机科学与技术学院　贵阳 550025
3 贵州大学密码学与数据安全研究所　贵阳 550025
4 贵州财经大学信息学院　贵阳 550025
(yxiny_gzu@163.com)

摘　要　拜占庭容错算法(byzantine fault-tolerant)是保证区块链等分布式系统能够达成一致性的重要算法,其性能影响着系统的安全性和稳定性。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,并分析证明信誉稳定策略的存在性,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的积极性。实验结果表明,所提共识算法可提升40%的吞吐量,且在共识过程中对节点所设计的信誉演化博弈模型有快速收敛的效果。

关键词:区块链;信誉机制;共识算法;激励机制;演化博弈
中图法分类号　O225

Rational PBFT Consensus Algorithm with Evolutionary Game

YANG Xin-yu[1,3],PENG Chang-gen[1,2,3],YANG Hui[1] and DING Hong-fa[4]
1 College of Mathematics and Statistics,State Key Laboratory of Public Big Data,Guizhou University,Guiyang 550025,China
2 College of Computer Science and Technology,Guizhou University,Guiyang 550025,China
3 Institute of Cryptography and Data Security,Guizhou University,Guiyang 550025,China
4 College of Information,Guizhou University of Finance and Economics,Guiyang 550025,China

Abstract　Byzantine fault-tolerant algorithm is vital to ensure the distributed system such as blockchain reaching consistency. The performance of algorithm affects the security and stability of the system. In view of the low efficiency and lack of incentive mechanism of existing consensus algorithms,a rational practical Byzantine fault-tolerant consensus algorithm with evolutionary game is proposed. Firstly,the trustworthiness of nodes in the consensus process is determined by node trust evaluation,the reputation value is used as the basis for the consensus enthusiasm of rational nodes,consensus nodes are divided based on reputation value,and the consensus method of node network fragmentation is adopted to improve consensus efficiency;secondly,the evolutionary game model is established for the impact of link dynamics between nodes in the consensus process on the reputation value,and based on the existence of the reputation stabilization strategy,an incentive mechanism based on reputation value rewards is designed to enhance the enthusiasm of consensus nodes to participate in consensus. Simulation results show that the consensus algorithm has a throughput increase of 40%,and the reputation evolution game model designed for nodes has a rapid convergence effect in the consensus process.

Keywords　Blockchain,Reputation mechanism,Consensus algorithm,Incentive mechanism,Evolutionary game

到稿日期:2021-09-13　返修日期:2022-01-05
基金项目:国家自然科学基金(U1836205);贵州省科技计划基金(黔科合平台人才[2020]5017);贵州省教育厅自然科学项目(黔教合KY字[2021]140);贵州大学培育项目([2019]56);贵州大学人才引进科研项目([2020]61)
This work was supported by the Natural Science Foundation of China(U1836205),Science and Technology Program of Guizhou Province(Qian-Science-Contract-Platform-Talent[2020]5017),Natural Science Fundation of Guizhou Provincial Education Department(Qian-Education-Contact-KY[2021]140),Cultivation Project of Guizhou University([2019]56) and Research Project of Guizhou University for Talent Introduction([2020]61).
通信作者:丁红发(hongfa.ding@foxmail.com)

1 引言

区块链作为一种分布式结构的数据库，融合了加密算法与签名方案、共识机制以及对等传输协议等多种技术，其以去中心化和透明、可溯源等特性，被广泛地应用于社会金融、互联网工业以及智能物联网等领域。共识算法是保证区块链系统达成一致性的核心算法，其中实用拜占庭容错算法(Practical Byzantine Fault-Tolerant，PBFT)[1]以其良好的容错性能和低耗能优势，成为了区块链共识机制领域的研究热点[2-4]。

由于分布式系统中节点交互行为的任意性，共识算法在执行过程中往往会受到恶意节点的影响，且共识算法本身的通信复杂度高且可扩展性不足等问题造成了系统性能低下[2]。PBFT 算法虽然针对恶意节点的容错阈值达到了系统节点总数的三分之一，但在实际应用中，共识性能除了受到恶意节点的影响之外，还与共识节点整体的积极性有关。因此，在基于实际需求的共识算法的实现过程中，如何在保证共识算法具有稳健执行性的前提下，结合机制提升算法相应的性能，具有重要的研究意义。

通过建立信誉机制来限制实际应用中区块链系统节点之间交互行为的任意性是非常可靠的[5]。对系统中的节点进行信誉属性的度量[6-8]，筛选出符合系统需求的良性节点进行共识，不仅能提升系统的安全性，还能节省系统因不必要共识产生的通信成本，大大提升了区块链系统的性能。在多方节点维护的区块链系统中，最佳效益的达成需要伴随着公平的收益分配，以信誉属性作为节点的共识策略来建立博弈模型[9]，分析各方在区块链系统中所提供的效益与所得收益之间的关系，并据此采取激励机制可保证方案对参与节点的公平性。

针对 PBFT 共识算法的综合性能低下的问题，Li 等[10]提出了一种网络分片的共识机制协议，对系统中的节点进行线性分割，但分片后的线性结构中并未加入对节点行为的度量机制，导致协议在恶意节点接近容错阈值时正确共识的成功率会陡然下降，这可能直接造成系统的瞬间瘫痪。且该方案并未给出具体节点状态更新的过程，遗留了原始 PBFT 算法中因视图频繁轮换导致算法性能低下的缺陷。针对系统中拜占庭节点恶意行为的问题，Xu 等[11]提出了结合信誉机制的改进容错共识协议，使得共识过程建立在信誉值较高的节点集中，以保证共识的安全性和效率。针对区块链系统扩展性能低下的问题，Lei 等[12]提出了一种信誉机制，用于评估参与节点的可信度，但该方案存在“马太效应”，使得节点信誉不断累计导致系统的中心化程度较高。针对共识节点信誉值演化的公平性问题，Biryukov 等[13]结合概率分布提出了一种相对公平的信誉模型方案，该方案通过信誉模型对共识节点的共识行为进行度量，而在共识过程中仍采用节点信誉值相关联的概率策略模型进行节点状态的转移。结合信誉机制改进 PBFT 算法的方案[14-15]中，通过采用设定信誉阈值对共识节点身份进行划分的方式，来保证共识机制的安全性，但该方案的可扩展性低，且缺乏共识节点之间动态交互对共识影响的分析。基于分片区块链系统，Yu 等[16]提出了一种包含信誉数据链的双链结构区块链系统，但是由于该系统采用基于算力的共识机制，因此其吞吐率较低且不环保，同时不能抵御长程攻击[17]。针对非许可链系统中的矿工收益分配问题，Manshaei 等[18]提出了结合非合作博弈的公平收益方案，该方案对“挖矿”行为进行策略性的博弈建模，并给出了一种较公平的利益分配方案，但该利益分配方案未从动态链路角度分析节点之间达成共识的积极效益，导致其不能很好地契合实际应用场景。在相关的结合演化博弈研究的文献中，Tian 等[19]结合博弈模型的安全协议提出了一种有效的安全协议博弈机制；基于演化博弈理论对节点之间的访问交互进行博弈建模的方案[20]，有效地解决了自适应访问控制中的隐私安全问题。

针对现有结合信誉机制的共识容错算法方案中存在信誉积累的问题[12-15]，本文设计了拥有初始值的信誉迭代机制，以权衡信誉机制在节点共识过程中的影响；针对文献[10]中容错性能不稳定的问题，依据所设计的信誉机制对恶意节点进行隔离，将共识成功率与正常共识节点的信誉值联立，使得算法在恶意比率上升的过程中平缓共识算法共识的成功率；针对现有共识容错算法缺乏适宜稳健性的方案，将信誉值作为参数指标，并提出了一种演化博弈模型下基于节点信誉的激励机制方案。

本文的主要贡献如下：

(1)提出了演化博弈模型下结合信誉机制的 PBFT 算法。采用对共识过程中因素的量化来对节点在共识阶段的投票行为进行精确度量，共识节点不同的信誉值表示在共识过程中节点对共识拥有不同程度的话语权；在主节点选取中增加随机性，使得共识机制更具公平性。

(2)结合信誉机制与策略稳定性，给出了共识算法的激励机制。同时提出从共识节点之间动态交互产生的链路变化角度来建立演化博弈模型，以节点之间的动态交互来分析有限理性下节点信誉值的演化并求解演化稳定策略，从而保证算法的稳健性。

(3)仿真分析表明，改进算法在信誉模型方面较现有算法[15-16]有明显的优势。所提算法相比文献[16]中的算法拥有将近 40%的吞吐量提升，并且所设计的基于信誉的激励机制以显著的收敛效果在提升共识成功率的同时还保证了算法的稳定性。

2 相关知识

本节介绍了 PBFT 算法的共识机理、群体博弈以及演化博弈相关理论知识，为面向改进共识算法的信誉机制模型与激励机制提供了理论基础。

2.1 PBFT 算法

PBFT 算法通过 3 个过程来实现，即客户端请求、共识过程、节点反馈。如果在最终反馈阶段收到超过$(m/3)$个不同节点的一致签名消息，则共识阶段输出的交易消息有效。而恶意节点阈值 $f_{malicious} \leqslant (m-1)/3$ 表示在系统中至少有一个诚实节点的情形下，PBFT 算法至多可容忍 $f_{malicious}$ 个恶意节点的任意行为。

共识算法的共识协议执行过程如图 1 所示，整个协议流程分为 5 个步骤。

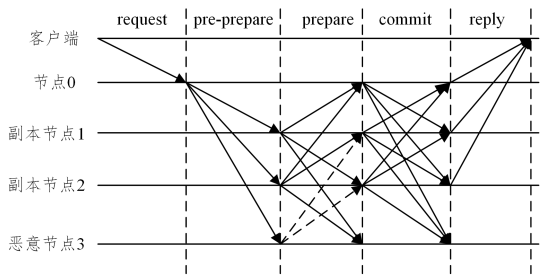


图 1 PBFT 算法的共识协议过程

Fig. 1 Consensus process in PBFT

Step 1 请求阶段。客户端向当前视图主节点发送请求消息〈request〉。

Step 2 共识预准备。主节点在收到〈request〉后，对请求序列进行排序，并将消息打包成预准备消息〈pre-prepare〉，在将消息添加至本地日志后，将其广播给系统中的其他共识节点。

Step 3 共识准备。系统中各共识节点在接收到来自主节点的预准备消息后，对消息进行正确性检验，在得到验证结果后，将消息添加至本地日志，并向系统中的其他共识节点广播〈prepare〉消息。

Step 4 共识提交。共识节点在接收到来自其他共识节点的〈prepare〉消息后，对消息的正确性进行验证，在将〈pre-pare〉消息和验证结果保存至本地日志后，向系统中的其他节点广播〈commit〉消息，并将其作为对当前〈prepare〉消息正确性的投票。

Step 5 反馈。通过共识准备阶段，主节点在收集到至少来自 $2f_{malicious}+1$ 个不同节点的一致性确认消息后，向客户端反馈〈request〉消息的共识结果。客户端收集到来自 $f_{malicious}+1$ 个不同节点的一致性确认结果后，共识协议进入下一轮执行。

PBFT 算法虽然资源损耗低且在容错性能以及节点通信等方面都有着良好的优势，但该算法采用的通信复杂度 $O(n^2)$ 较高，而且算法的可扩展性有限。因此，优化算法的复杂度并在保证安全的前提下提升算法的可扩展性具有重要的研究意义。

2.2 演化博弈理论

2.2.1 群体博弈模型理论的形式化定义

定义 1(群体博弈模型[21]) 群体博弈模型可形式化表示为一个四元组：

$$E^p=\{N^p,SR^p,\Delta^{NE},U^p\} \tag{1}$$

其中，参数符号的含义如表 1 所列，表 1 中参数内容对应参数具体的数学含义。

表 1 群体博弈模型参数符号释义

Table 1 Parameter symbol interpretation of population games

参数符号	参数内容	参数含义
N^p	$\{1,2,\cdots,p\}$	种群数量
SR^p	$\{s^p\in R_+^{n^p}:\sum s_j^p=m^p,j\in ST^p\}$	种群状态
$\Delta^{NE}(U^p)$	—	纳什平衡策略集
U^p	$\{U_i^p:i\in SR^p,p\in N^p\}$	收益函数

2.2.2 演化博弈论形式定义

定义 2(演化博弈模型[21]) 演化博弈模型在群体博弈上形式化表示为：

$$G^p=\{E^p,\rho_{ij}^p(U^p,s^p),\Delta^{ESS}\} \tag{2}$$

其中，相应的参数符号的含义如表 2 所列。

表 2 演化博弈模型参数释义

Table 2 Parameter interpretation of evolutionary dynamics

参数符号	参数内容	参数含义
E^p	—	群体博弈模型
ρ_{ij}^p	$\rho_{ij}^p(U^p,s^p)(i,j\in ST^p)$	策略转移概率
s^p	—	演化稳定策略
Δ^{ESS}	—	演化稳定策略集

群体博弈理论中，各方参与者通过执行当前时间下策略集中的策略来获得收益，在重复进行策略选择的过程中，参与者之间会进行“模仿”，趋向于选择高收益回报策略，当选择策略趋于稳定时，便可得到演化稳定策略集。

定义 3(演化稳定策略集[21]) 策略集的定义为：

$$s^p(s^p\in\Delta^{ESS}\subseteq\Delta^{NE}) \tag{3}$$

2.2.3 演化博弈动态

演化博弈中，对动态决策机制的刻画对应于平均动态微分方程，它能够在演化周期 T 内精确地将有限理性参与者的行为动态变化过程描绘出来，具体指，在某一周期中的时刻 t，某一纯策略选择带来的收益与从该策略转移到其他策略获得的收益之差。

定义 4(演化博弈动态[21]) 具体的动态微分方程为：

$$\dot{s}_i^p=\sum_{j=1}^{n^p}s_j^p\rho_{ji}^p(U^p,s^p)-s_i^p\sum_{k=1}^{n^p}\rho_{ik}^p(U^p,s^p) \tag{4}$$

其中，$i,j,k\in N^p$ 为种群个体。

3 PBFT 算法的改进

本文在 PBFT 算法的基础上进行改进，添加了信誉机制模型和激励机制，并基于公平性引入随机性的主节点集选取，在安全性的前提下保证所提方案的稳健性。具体的研究方案框架如图 2 所示。

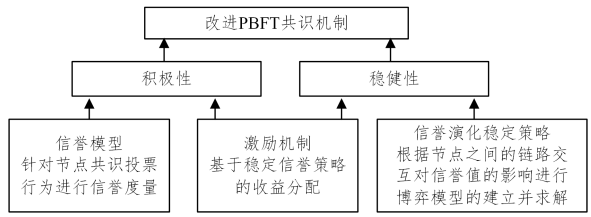


图 2 本文研究结构框架

Fig. 2 Research framework of this scheme

首先，基于 PBFT 算法中的投票共识设计信誉机制模型，主要针对节点对区块共识的积极性进行评估，从而进行信誉的确定；然后，通过对信誉机制模型中的投票行为进行博弈建模，将共识积极性关联到节点交互的链路收益中，证明信誉机制模型下节点信誉值演化的稳定性；最后，依据所得的具有演化稳定性的信誉值来设计共识算法的激励机制，以保证系统的稳健性。

3.1 信誉机制

设计的信誉机制模型综合共识投票过程中的因素，对节点的信誉进行评估，具体考虑以下重要因素：

(1)共识阶段节点之间的交互、反馈；

(2)周期 T 中主节点收集到的交易事务量性，如交易大小、交易数量等；

(3)节点在周期 T 期间的共识投票行为；

(4)系统的稳健性以及外部扩展状态。

涉及到的参数为：

1)共识周期 t 后共识节点 i 的直接信任值 α_i^t；

2)共识周期 t 前收集到的事务集数量值 tx_t，以及该周期后成功被添加到区块链中的事务数量值 tx_t^p；

3)共识周期 t 内的共识次数 m_t，以及总共识成功次数 m_t^h $(0\leqslant m_t^h\leqslant m_t)$；

4)共识周期 t 内，节点 i 认同共识过程中主节点集发布区块 $B_{t,k}$ 的正确性($B_{t,k}$ 最终被添加至链上)次数 τ_i^t，以及反对区块 $B_{t,k}$ 的正确性次数 v_i^t。

首先给定节点初始信誉值 α_i^0，通过共识周期的更迭来更新节点的信誉值，通过量化共识预准备阶段之前所收集到的事务集来表示共识阶段的重要程度，旨在区分关键型的事务集和非关键型事务集的数量比重对节点共识的影响，同时利用 Sigmoid 型函数的良好特性，将节点信誉值控制在[0,1]范围内，以便信誉阈值策略的设定。相应节点的直接信誉值的定义如下。

定义 5(节点的直接信誉值) 节点 i 在共识周期 t 完成后的信誉值为：

$$\alpha_i^t=1-\frac{2\mathrm{e}^{-\frac{tx_t^p}{tx_t}\left(\frac{m_t^h}{m_t}\tau_i^t-v_i^t\right)}}{\alpha_i^0+\mathrm{e}^{-\frac{tx_t^p}{tx_t}\left(\frac{m_t^h}{m_t}\tau_i^t-v_i^t\right)}} \tag{5}$$

系统节点自由加入和退出使得节点的链接具有动态性，假设节点按照密度参数为 λ 的泊松过程分布在图 3 所示的拓扑图中，给定节点覆盖半径为 R(或 r)内所有节点的信息。基于文献[22]设计了一种信誉传播计算方法，使得在共识过程中两个节点中的一方或者双方在本地未存储对方信息的情形下进行基于信誉值的交互。

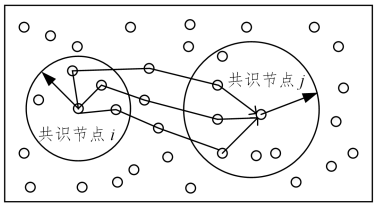


图 3 动态链接拓扑下的间接信誉传播

Fig. 3 Reputation communication based on dynamic topology

本文采用修正余弦函数来衡量节点之间的信誉值相似度，以定义节点之间的间接信誉值，具体定义如下。

定义 6(节点的间接信誉值) 节点 i 相对于节点 j 的间接信誉值为 $\alpha(i\rightarrow j)$，具体表达式为：

$$\alpha^t(i\rightarrow j)=\frac{\sum\limits_{k\in I}\left[sim^t(i,k)\cdot\alpha_i^t\right]}{\sum\limits_{k\in I}sim^t(i,k)} \tag{6}$$

其中，$\sum sim^t(i,k)$ 表示信誉传播路径中的节点与节点 i 的相似度之和，具体的表达式如下：

$$sim^t(i,k)=\frac{\sum\limits_{\|i\wedge h\|}|\alpha_{i\wedge h}^t-\overline{\alpha_i^t}|\cdot\sum\limits_{\|k\wedge h\|}|\alpha_{k\wedge h}^t-\overline{\alpha_k^t}|}{\sqrt{\sum\limits_{i\wedge h}(\alpha_{i\wedge h}^t-\overline{\alpha_i^t})^2}\cdot\sqrt{\sum\limits_{k\wedge h}(\alpha_{k\wedge h}^t-\overline{\alpha_k^t})^2}}$$

其中，$x\wedge h$ 表示当前阶段信誉值传播过程中与节点 x 有交互历史的节点，且 h 与节点 x 都有相应的共识节点交集；$\overline{\alpha_i^t}$ 表示节点 i 直至 t 时的历史平均信誉值。

通过综合推荐路径中节点信誉值的权重和信誉值的相似度来定义间接信誉值，使得系统扩展过程中加入的新节点更多地被考虑到机制中。

3.2 节点状态更新

本文改进的 PBFT 算法利用节点信誉值进行主节点的更新，对节点进行分层随机性的选举，从信誉值降序分层的节点集中选取主节点，结合信誉值的更新机制来实现随机性公平的选举。

图 4 给出了节点状态更新的流程，其中共识节点与主节点之间的状态通过随机化进行转换，共识节点跟随主节点完成共识并监督主节点的诚实性。而具体的更新规则为上级节点状态更新和共识节点状态更新。

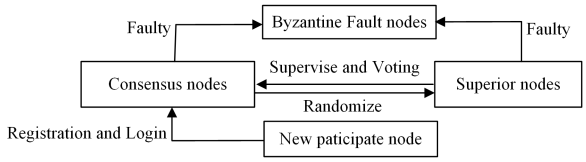


图 4 节点状态更新

Fig. 4 Switching of nodes state

(1)上级节点状态更新

$$\begin{cases}\{Sn\leftrightarrow Cn\}:random\begin{Bmatrix}order_{descend}^{1,n}(\alpha_{Cn})\\ \cdots\\ order_{descend}^{m,n}(\alpha_{Cn})\end{Bmatrix}\\ \{Sn\rightarrow BFn\}:Sn\in\begin{Bmatrix}f_{malicious}\\ \|\ Sn\xrightarrow{\inf}receiver=error\end{Bmatrix}\end{cases}$$

其中，

$$\begin{Bmatrix}order_{descend}^{1,n}(\alpha_{Cn})\\ \cdots\\ order_{descend}^{m,n}(\alpha_{Cn})\end{Bmatrix}$$

表示系统中的 mn 个共识节点根据声誉值按降序排序分组，共计 m 组中每组 n 个节点。

图 5 为共识节点层次结构的示意图。改进后的 PBFT 共识算法将共识节点分为主节点集与共识节点组，各共识组同步独立运行共识机制，由该组主节点引导共识的进程。图 5 中，上层为主节点集，下层为共识节点群组，其中主节点有 m 个，且分别对应于 m 个共识节点群组。

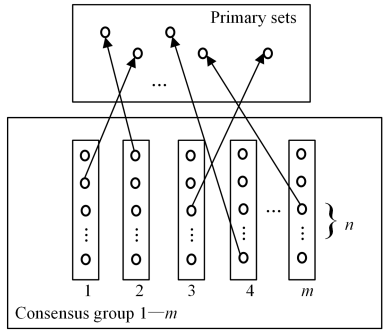


图 5 共识节点层次结构

Fig. 5 Structure of consensus nodes

在共识周期完成后，需要从信誉值降序排列的 mn 个共识节点中随机选出 m 个上级节点。首先从信誉值降序序列前 n 个共识节点中随机选取第一个上级节点，然后依次从剩余信誉值降序序列中随机选出上级节点。当上级节点在系统中广播错误消息时，诚实节点通过对共识消息的验证，标记出该上级节点是拜占庭错误节点，并执行共识节点状态更新。

(2)共识节点状态更新

$$\begin{cases}\{Cn\rightarrow BFn\}:Cn\in\left\{\begin{array}{c}f_{malicious}\\ \| Cn\xrightarrow{\inf} receiver=error\end{array}\right\}\\ \{Npn\rightarrow Cn\}:Npn\in\left\{\begin{array}{c}\alpha_{Npn}=\alpha_0\\ ID_{f_{malicious}}\notin topol\_table_{Npn}\end{array}\right\}\end{cases}$$

当共识节点在系统中广播错误消息时，诚实节点接收并验证该消息后从本地路由表中删除该节点的路由信息，并一致标记该节点为拜占庭错误节点。系统默认新参与节点信誉值为 α_0，且新参与节点不能立即参与共识过程，在下一轮共识开始前，新参与节点同步系统状态并标记相应拜占庭错误节点。

当诚实节点接收到主节点集中的恶意行为消息时，针对当前主节点集发起主节点更新请求并广播至系统内的各节点，主节点集接收到请求后验证请求正确性，若正确，则按照上述节点选取机制进行主节点更换，被选定的节点在收到至少来自 $f_{malicious}+1$ 个不同节点的一致确认消息后，将被添加至主节点集，并当选为下一轮共识主节点集合中的主节点。图 6 给出了主节点更新协议的具体流程。

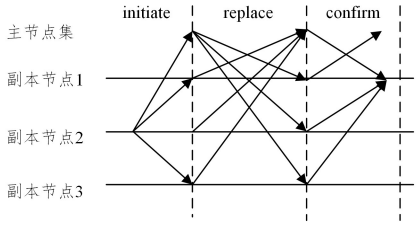


图 6 主节点更新流程

Fig. 6 Process of primary node

主节点更新算法如算法 1 所示。算法 1 依据节点的信誉值进行主节点的选取与确认，首先针对恶意主节点的替换达成共识，然后依据节点的信誉值随机选取新的主节点。

算法 1 主节点更新算法

输入：错误主节点 s_p，正常共识节点 i，节点 i 的共识信誉值 α_i，错误共识消息 message=error

输出：新主节点集合列表 primary−list，主节点更新替换消息集[primary−replace]，更新后主节点信誉值列表[α_{s-list}]

1. 共识节点收到当前视图中主节点集合中发送错误消息的节点，向其他节点发送该主节点恶意行为的证明并发起主节点更换请求消息，消息内容为：

   $\langle$primary−replace$\langle s_p$,message=error$\rangle_{\sigma_p}$,α_i,i,digest$\rangle_{\sigma_i}$

   其中，σ 表示相应节点的签名信息。

2. 当至少 $f_{malicious}+1$ 个不同共识节点一致确认主节点恶意行为后，主节点集合通过随机机制选取新的主节点并广播主节点更换消息。

   $\langle$primary−replace−confirm α_j,j,digest$\rangle_{\sigma_s}$

   其中，j 表示当选主节点的共识节点序号，α_j 表示该预主节点对应的信誉值。

3. 节点 j 更新并收集是否有 $2f_{malicious}+1$ 个不同共识节点发送更新主节点更换消息，若有，则节点 j 向主节点集合发送主节点确认消息。

   $\langle$primary−confirm[$num_{confirm}\rangle 2fmalicious+1$],$\alpha_j$,j,digest$\rangle\sigma_j$

   并执行步骤 4；否则直接结束。

4. 主节点集合更新视图的主节点集合，并向系统中共识节点发送主节点更新完成消息。

   $\langle$primary−list[primary−replace],[α_{s-list}],digest$\rangle_{\sigma_s}$

3.3 PBFT 算法的改进

图 7 给出了改进的 PBFT 算法的共识协议过程。其中，主节点集合以{0}表示，并且主节点集参与共识的投票过程。改进 PBFT 算法除了对主节点进行集合化提升效率外，还依据信誉机制的节点共识相应减少原先 PBFT 算法中 commit 阶段的通信次数。

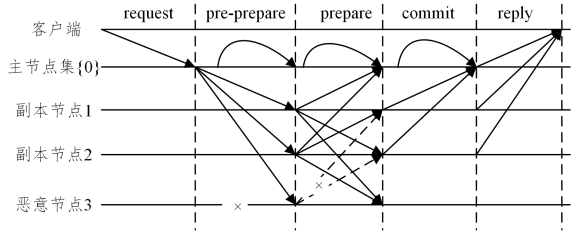


图 7 改进的 PBFT 算法的共识协议过程

Fig. 7 Consensus process of improve PBFT

改进的 PBFT 算法如算法 2 所示。算法 2 中节点的交互过程增加了节点信誉值的交换，即达到设定信誉阈值的节点才有相应程度的共识话语权。

算法 2 改进 PBFT 算法

输入：当前共识系统状态；交易信息集 Tx_{client}

输出：本轮共识一致性结果；新的共识系统状态

1. request 阶段：客户端 client 将 Tx_{client} 发送给当前视图下的主节点集{0}。主节点集中节点在接收到 Tx_{client} 后验证其中交易 tx_i($tx_i\in Tx_{client}$)的有效性，将有效的交易集$\{tx_i\}$打包至新区块中，并生成可在 merkle tree 中检索到的块头信息 $Block_{head}$。

2. pre-prepare 阶段：当前视图主节点集{0}广播预准备消息(pre-prepare)至系统中的各共识节点，而 pre-prepare 主体形式为：

   $\{\langle$pre-prepare,$num_{v,r}$,$topol_0$,digest$\rangle\}_{\sigma_0}$

   其中，num_v 表示当前视图的编号值，num_r 表示 requst 消息的序列值，$topol_0$ 表示主节点集{0}所存储的共识节点信息表(其中包含节点的信誉值等信息)，σ_0 表示主节点集签名信息，而 digest 表示信息的摘要。

3. prepare 阶段：当前视图下共识节点 1,2,3 在收到来自主节点集{0}发送的 pre-prepare 消息后，先验证消息的正确性，若正确性通过，则向系统中其他共识节点发送准备消息(prepare)，prepare 的形式为：

   $\{\langle$prepare,num_v,$topol_i$,$drop_i$,digest$\rangle\}_{\sigma_i}$

4. commit 阶段：当前视图下其他共识节点在收到 prepare 消息后，计算消息源节点的直接信誉值 α_i(或间接信誉值)。当 $\alpha_i\geqslant\alpha_k$ 时，共识节点更新本地共识节点列表以及区块状态信息，并发送提交消息至主节点集(commit)，commit 的形式为：

   $\{\langle$commit,num_v,$topol_i$,$drop_i$,digest$\rangle\langle$reputation_table$_i\rangle\}_{\sigma_i}$

5. reply 阶段：在提交阶段完成后，当前视图共识节点在本地更新当前

的系统状态，主节点集中的节点将针对新区块的共识输出结果回复给客户端，并对当前视图中的共识节点进行基于信誉值的排序，在正常信誉值阈值以外的节点将被隔离出共识过程。在达到预设共识周期轮数后，主节点集完成了激励机制，共识进入下一轮周期。

4 基于演化博弈模型的共识算法激励机制

本节从共识机制中节点之间的动态链接交互对节点信誉值进行演化博弈模型的建立。通过相关收益函数的建立，分析节点信誉值演化的稳定性并以此建立激励机制，保证了算法的稳健性。

4.1 改进的 PBFT 共识中的演化博弈模型

本文通过节点之间链接与断开的动态过程，对信誉值的变化进行稳定性分析，旨在通过演化博弈理论来分析共识过程中节点之间交互对信誉值的影响。其中诚实共识节点为了获取高的信誉值会选择最佳的投票行为策略，并根据该策略行为对应的收益来学习更高收益节点的策略行为。

定义 7（演化博弈模型） 基于信誉机制的共识节点链路演化博弈模型（Evolutionary Game Model of Consensus Node Link Based on Reputation Mechanism，EMCNLBR）的形式化定义为：

$$EMCNLBR=\{N,S,\xi,Q,\rho_{ij},\Delta^{ESS},\Delta^{t}_{state}\} \tag{7}$$

EMCNLBR 中相关参数的符号含义如表 3 所列。表 3 中包括博弈的主体、博弈策略以及与策略相对应的收益函数。

表 3 EMCNLBR 符号释义

Table 3 Symbol interpretation of EMCNLBR

参数符号	参数内容	参数含义
N	$\{1,2,\cdots,n\},n\in N+$	共识节点集
S	$\{S^{pure},S^{mixed}\}$	节点信誉策略
Δ^{t}_{state}	—	稳定策略集

表 3 中，结合信誉机制计算出来的信誉数值 $\alpha_i^t\in S$，$S^{pure}=[0,\alpha_{\max}]$表示纯策略集合，$S^{mixed}$表示混合策略集合。

4.1.2 EMCNLBR 模型中的相关定义

（1）节点之间的拓扑链接结构

定义 8（节点关系[23]） 区块链系统中任意两节点 i,j 之间的关系定义为：

$$r_{ij}=\begin{cases}1, & \text{if } (i,j) \text{ connected}\\ 0, & \text{otherwise}\end{cases} \tag{8}$$

本文中关于任意节点之间的关系是对称的，即区块链系统中节点连接形成的拓扑结构图的邻接矩阵 $\boldsymbol{A}(\boldsymbol{A}\in\Re^{n\times n})$是对称矩阵，且 $\boldsymbol{A}$ 中对角元素全为零，即 $r_{ij}=0$。

定义 9（节点连通度[23]） 区块链系统中与任意共识节点 $i\in N$ 连接的节点总数为：

$$d^{i}_{Num}=degree_{Num}(node_i) \tag{9}$$

其中，d^{i}_{Num}表示节点 $i\in N$ 与系统中其他节点通过路由表或者 $ID(node)$建立链接的个数，通过图论中点的度值（Degree）来定义。由定义 8 可知，本文中节点 $i\in N$，出度值 d^{i}_{OutNum}与入度值 d^{i}_{InNum}相同。

（2）节点链路适应函数与收益函数

正常共识节点的链接关系总是为共识机制的完成起到积极的作用。本文基于此将链路适应函数分为静态与动态，静态情形为该节点与其他节点链接适应度以及因链接所产生的成本加和表示；动态情形下，节点在 $t\in T$ 时不仅依靠当下链接的节点来获得适应度收益，同时还与产生新链接关系的节点有关。基于文献[23]中节点链路适应度的定义，本文给出节点的链接适应函数，具体的定义如下。

定义 10（静态链路适应函数和动态链路适应函数） 定义静态链路适应函数 $U(\alpha_i^t)$为：

$$U(\alpha_i^t)=p\sum_{l=1}^{n}r_{il}\alpha_l^t-qd^{i}_{Num}\alpha_i^t \tag{10}$$

其中，$p>q>0$。

定义动态链路适应函数 $D(\alpha_i^t)$为：

$$D(\alpha_i^t)=\sum_{k=1}^{n}r_{ik(creat)}\alpha_k^t \tag{11}$$

其中，$r_{ik(creat)}$表示节点 k 与节点 i 建立新链接。相应的链路变化总适应函数为：

$$Q(\alpha_i^t)=D(\alpha_i^t)+U(\alpha_i^t) \tag{12}$$

$$Q(\alpha_i^t)=p\sum_{l=1}^{n}r_{il}\alpha_l^t-qd^{i}_{Num}\alpha_i^t+\sum_{k=1}^{n}r_{ik(creat)}\alpha_k^t \tag{13}$$

定义 11（节点链路状态总收益函数 F） 用 F 表示节点在系统中链路状态的总收益函数，在链路适应函数的基础上，本文采用式(14)所示的收益向量函数。

$$F:[F_i=[D(\alpha_i^t)+U(\alpha_i^t)]\cdot\alpha_i^t] \tag{14}$$

（3）模型形式化

本文以链路适应性对系统中的节点进行演化模型的建立，并使用 Sigmoid 函数对策略转移概率进行形式化的定义，相应定义为：

$$\rho_{ij}=sig(\eta\cdot\Delta F_{ij})=\frac{1}{(1+\mathrm{e}^{-\eta\Delta F_{ij}})} \tag{15}$$

$$\rho_{ij}=\frac{\mathrm{e}^{-\eta F(\alpha_i^t)}}{(\mathrm{e}^{-\eta F(\alpha_j^t)})+\mathrm{e}^{-\eta F(\alpha_i^t)})}=\frac{1}{(1+\mathrm{e}^{-\eta\Delta F_{ij}})} \tag{16}$$

式(15)、式(16)中，ρ_{ij}为策略转移概率，其中：

$$\begin{aligned}\Delta F_{ij}:&=F_i(\alpha_i^t)-F_j(\alpha_j^t)\\&=[D(\alpha_i^t)+U(\alpha_i^t)]\cdot\alpha_i^t-[D(\alpha_j^t)+U(\alpha_j^t)]\cdot\alpha_j^t\end{aligned} \tag{17}$$

其中，$\eta>0$ 表示系统的噪声因子。由式(17)可以看出，ΔF 越大，转移概率就越接近 1。

由式(4)、式(8)－式(10)、式(15)、式(17)可得，EMCNLBR 的微分方程为：

$$\begin{aligned}\dot{\alpha}_i(t)&=\frac{1}{d^{i}_{Num}}[\sum_{l=1}^{n}\alpha_l(t)r_{il}\rho_{li}-\alpha_i(t)\sum_{k=1}^{n}r_{ik}\rho_{ik}]\\&=\frac{1}{d^{i}_{Num}}[\sum_{k=1}^{n}\alpha_k(t)r_{ik}(1-\rho_{ik})-\alpha_i(t)\sum_{k=1}^{n}r_{ik}\rho_{ik}]\\&(\rho_{ij}+\rho_{ji}=1)\end{aligned} \tag{18}$$

4.2 演化均衡策略的存在性与稳定性

4.2.1 EMCNLBR 中纳什均衡的存在性

定理 1 EMCNLBR 中存在纳什均衡。

证明：EMCNLBR 模型的策略空间集定义在$[0,\alpha_{\max}]$上，因此 EMCNLBR 模型中的策略空间集合是欧氏空间上非空的有界闭凸集合。

$$\begin{aligned}F(\alpha_i^t)&=[D(\alpha_i^t)+U(\alpha_i^t)]\cdot\alpha_i^t\\&=[p\sum_{l=1}^{n}r_{il}\alpha_l^t-qd^{i}_{Num}\alpha_i^t+\sum_{k=1}^{n}r_{ik(creat)}\alpha_k^t]\cdot\alpha_i^t\\&=(p\sum_{l=1}^{n}r_{il}\alpha_l^t)\cdot\alpha_i^t-qd^{i}_{Num}(\alpha_i^t)^2+(\sum_{k=1}^{n}r_{ik(creat)}\alpha_k^t)\cdot\alpha_i^t\end{aligned}$$

若考虑 F 在 R 上是连续的，则收益函数 $F(\alpha_i^t)$ 对 α_i^t 的一阶偏微分为：

$$\frac{\partial F(\alpha_i^t,\alpha_{-i}^t)}{\partial \alpha_i^t}=[D(\alpha_i^t)+U(\alpha_i^t)]-qd_{Num}^i\alpha_i^t$$
$$=Q(\alpha_i^t)-qd_{Num}^i\alpha_i^t$$

则由可微函数中一阶优化的必要性可知，令：

$$\frac{\partial F(\alpha_i^t,\alpha_{-i}^t)}{\partial \alpha_i^t}=0$$

则由极大值定理可得：

$$(\alpha_i^t)^*=\frac{p\sum_{l=1}^{n}r_{il}\alpha_l^t+\sum_{k=1}^{n}r_{ik(creat)}\alpha_k^t}{2qd_{Num}^i},i\in N$$

收益函数 $F(\alpha_i^t)$ 对 α_i^t 的二阶偏微分为：

$$\frac{\partial^2 F(\alpha_i^t,\alpha_{-i}^t)}{\partial \alpha_i^{t2}}=-qd_{Num}^i<0$$

因此，收益函数 $F(\alpha_i^t,\alpha_{-i}^t)$ 在 R 上具有凹性，则由上述证明过程与文献[24]所给的纳什均衡定义可知，EMCNLBR 中存在纳什均衡。

4.2.2 EMCNLBR 中纳什均衡的稳定性

利用式(18)刻画共识系统中节点信誉值的动态变化，便可得到关于系统中节点信誉变化的动态微分方程组。

$$\dot{\alpha}(t)=M(\alpha(t))=J\boldsymbol{H}(\alpha(t))\alpha(t)$$

其中，

$$J=(d_{Num}^1)^{-1},(d_{Num}^2)^{-1},\cdots,(d_{Num}^n)^{-1}]^{\mathrm{T}}$$

$$\boldsymbol{H}(\alpha(t))=\begin{bmatrix}-\sum_{k=1}^{n}\rho_{1k}r_{1k} & (1-\rho_{12})r_{12} & \cdots & (1-\rho_{1n})r_{1n}\\ \rho_{12}r_{21} & -\sum_{k=1}^{n}\rho_{2k}r_{2k} & \cdots & \rho_{n2}r_{2n}\\ \vdots & \vdots & \ddots & \vdots\\ \rho_{1n}r_{n1} & \rho_{2n}r_{2n} & \cdots & -\sum_{k=1}^{n}\rho_{nk}r_{nk}\end{bmatrix}$$

定理 2 EMCNLBR 中纳什均衡是稳定的。

证明：假定所有节点的度相同，即 $d_{Num}=d$ 固定。若 $\alpha^*\in[0,\alpha_{\max}]$ 是 EMCNLBR 模型中的纳什均衡点，则有：

$$\Delta F(\alpha_j)=F(\alpha_j^*)-F(\alpha_j)\geqslant 0$$

即收益向量在此状态下的策略转移概率指向均衡策略恒为正。

对于矩阵 $\boldsymbol{H}(\alpha(t))$ 利用 Jacobian 矩阵分析法，首先求解 $\boldsymbol{H}(\alpha(t))$ 中各个元的偏微分，即：

$$\frac{\partial(-\sum_{k=1}^{n}\rho_{ik}(\alpha^*)r_{ik})}{\partial\alpha_i}=-\sum_{k=1}^{n}[r_{ik}\rho_{ik}(1-\rho_{ik})\cdot((1+p)r_{ij}+qd_{Num})]$$
$$=-\frac{1}{4}\eta\sum_{k=1}^{n}r_{ik}((1+p)r_{ij}+qd_{Num})$$

$$\frac{\partial(\rho_{ij}(\alpha^*)r_{ji})}{\partial\alpha_j}=-r_{ij}\rho_{ij}(1-\rho_{ij})\cdot((1+p)r_{ij}+qd_{Num})$$
$$=-\frac{1}{4}\eta r_{ij}\cdot((1+p)r_{ij}+qd_{Num})$$

则可得矩阵 $\boldsymbol{H}(\alpha(t))$ 的 Jacobian 矩阵为：

$$\frac{1}{4}\eta\begin{bmatrix}-\sum_{k=1}^{n}r_{1k}[(1+p)r_{1k}+qd] & \cdots & -r_{1n}\cdot[(1+p)r_{1n}+qd]\\ \vdots & \ddots & \vdots\\ -r_{n1}\cdot[(1+p)r_{n1}+qd] & \cdots & -\sum_{k=1}^{n}r_{nk}[(1+p)r_{nk}+qd]\end{bmatrix}$$

对于任意非零实值列向量 $\boldsymbol{\beta}\in\Re^{n\times 1}$，记 $\boldsymbol{H}(\alpha(t))$ 的 Jacobian 矩阵为 $J_{H(\alpha(t))}$。

$$\boldsymbol{\beta}=[\boldsymbol{\beta}_1,\boldsymbol{\beta}_2,\cdots,\boldsymbol{\beta}_n]^{\mathrm{T}}$$

有：

$$\boldsymbol{\beta}^{\mathrm{T}}\boldsymbol{J}_{\boldsymbol{H}(\alpha(t))}\boldsymbol{\beta}=\frac{1}{4}\eta\begin{bmatrix}-\sum_{k=1}^{n}r_{1k}[(1+p)r_{1k}+qd](\beta_1+\beta_j)\\ \vdots\\ -\sum_{k=1}^{n}r_{nk}[(1+p)r_{nk}+qd](\boldsymbol{\beta}_n+\boldsymbol{\beta}_j)\end{bmatrix}^{\mathrm{T}}\begin{bmatrix}\boldsymbol{\beta}_1\\ \boldsymbol{\beta}_2\\ \vdots\\ \boldsymbol{\beta}_n\end{bmatrix}$$
$$=-\frac{1}{4}\eta\sum_{k=1}^{n}\sum_{j=1}^{n}r_{jk}[(1+p)r_{jk}+qd](\boldsymbol{\beta}_k+\boldsymbol{\beta}_j)^2<0$$

即证 $\boldsymbol{J}_{\boldsymbol{H}(\alpha(t))}$ 是负定矩阵且对应的特征值都是负数，即纳什均衡 $\alpha^*\in[0,\alpha_{\max}]$ 是 EMCNLBR 中的稳定纳什均衡点[25]。

4.2.3 稳定的激励机制设计

基于信誉稳定策略的存在性，通过奖励激励机制对共识节点进行激励，旨在提高系统中共识节点参与共识的积极性。

基于信誉策略的激励机制如算法 3 所示。

算法 3 基于演化稳定信誉策略的激励机制算法

输入：信誉值表 reputation_table，系统总收益 $\theta_{\mathrm{reward}}\cdot(\mathrm{tx}_{\mathrm{T}}^{\mathrm{p}})$，权重参数 ω

输出：共识节点收益 f^{i}，主节点收益值 f^{sp}，$\mathrm{topol\_table_i}$，$\mathrm{drop\_table_i}$

1. 首先主节点更新 reputation_table，对当前共识节点进行排序并统一更新节点状态信息表，再将其广播给系统中的其他节点进行确认。
2. 主节点收到 m 个共识节点的确认回复后，根据以下分配函数进行奖励分配。

副节点的收益分配函数为：

$\omega[\theta_{\mathrm{reward}}\cdot(\mathrm{tx}_{\mathrm{T}}^{\mathrm{p}})]$：

$$\mathrm{f}^{\mathrm{i}}=\begin{cases}0,\alpha_{\mathrm{i}}\leqslant\alpha_{\min}^{\mathrm{follower}}\\ \dfrac{\alpha_{\mathrm{i}}}{\sum_{\mathrm{j}\in\mathrm{j}_{\mathrm{follower}}}\alpha_{\mathrm{j}}},\alpha_{\min}^{\mathrm{follower}}<\alpha_{\mathrm{i}}\leqslant\alpha_{\max}^{\mathrm{follower}}\end{cases}\tag{19}$$

主节点的收益分配函数为：

$(1-\omega)[\theta_{\mathrm{reward}}\cdot(\mathrm{tx}_{\mathrm{T}}^{\mathrm{p}})]$：

$$\mathrm{f}^{\mathrm{sp}}=\frac{\alpha_{\mathrm{i}}}{\sum_{\mathrm{j}\in\mathrm{j}_{\mathrm{follower}}}\alpha_{\mathrm{j}}},\alpha_{\min}^{\mathrm{sp}}\leqslant\alpha_{\mathrm{i}}\leqslant\alpha_{\max}^{\mathrm{sp}}\tag{20}$$

3. 输出 f^{i} 和 f^{sp} 相应的值，系统中的共识节点基于 reputation_table，同步更新本地 topol_table 和 drop_table；正常共识节点标记恶意节点并断开与恶意节点的链接，以保持良性的拓扑链接状态。

算法 3 中各值代表的含义如下：

(1)$topol\_table_i$ 用于存放与节点 i 在共识阶段交互的节点信息、节点 i 与目标节点的拓扑距离、节点在共识周期内参与共识的次数以及参与共识正确性的次数、是否采用演化稳定策略 ESS 以及节点自身的链路收益；

(2)$drop\_table_i$ 用于存放与节点 i 断开链接的节点信息，并在共识阶段广播给其他节点；

(3)$reputation\_table_i$ 用于存放与节点 i 进行交互的相关节点信誉值。

5 安全性与性能分析

5.1 通信成本分析

改进 PBFT 共识机制的通信次数为 $m(n^2+m-2)$。

假设系统中有 mn 个节点，其中有 m 个主节点，其余 $m(n-1)$个为共识节点。

(1)客户端向主节点集中的节点发送请求消息，节点在收到请求消息后在主节点集中进行预准备阶段消息共识，该阶段的通信次数为 $m(m-1)$；

(2)在预准备阶段，主节点集中的节点向所在节点组广播预准备消息，该阶段的通信次数为 $m(n-1)$；

(3)在准备阶段，各节点组独立验证共识消息，该阶段的通信次数为 $m(n-1)^2$；

(4)在提交阶段，主节点集合中的节点接收共识节点的验证消息并进行验证，该阶段的通信次数为 $m(n-1)$。

因此，改进的 PBFT 共识算法的通信次数为 $m(n^2+m-2)$，同节点数目下原 PBFT 共识算法的通信次数为 $2mn(mn-1)$，而当 $1<m\ll n$ 时，有：

$$m(n^2+m-2)<2mn(mn-1)$$

虽然改进共识算法的通信复杂度仍为 $O(n^2)$，但结合信誉机制的共识算法会使通信次数大大降低。

5.2 改进的 PBFT 算法的安全性、一致性与活性

5.2.1 安全性分析

改进的 PBFT 共识依靠 PBFT 共识中各共识节点之间交互消息中的签名、时间戳保证了消息的安全性，而视图中共识协议的完整性限制节点不能进行超过当前视图编号的共识，保证了共识执行的安全性。

同时，改进的 PBFT 共识通过信誉机制对共识节点按照信誉值进行分片，使得各组内的节点拥有与共识相匹配的信誉度，通过限制低信誉度节点参与共识的权利以及剔除劣性信誉值的节点，来保证组内与组间共识节点的可靠性与安全性。根据 3.1 节信誉机制中的信誉策略可知，节点的信誉度表示对节点共识过程中共识行为的评价，而偏离共识协议节点的共识行为具有任意性，因此本文所设计的信誉机制具有对抗拜占庭节点恶意共识行为的能力。

通过上述分析可知，本文设计的方案能够在安全性的前提下输出正确共识结果。

5.2.2 一致性分析

改进的 PBFT 共识在 PBFT 共识的基础上实现了共识的一致性，并通过信誉机制对节点在共识过程中的投票行为进行了评估，保证了协议方案共识输出结果的一致性。改进的 PBFT 共识过程中，在容错阈值 $f_{malicious}\leqslant(m-1)/3$ 以内，主节点集合通过正常执行 PBFT 协议达成区块共识的一致性。同理，组内节点在阈值 $f_{malicious}\leqslant(n-1)/3$ 时，组内共识节点也可以正常执行 PBFT 协议来保证共识输出结果的一致性。在改进的 PBFT 共识协议执行的过程中，信誉机制会对执行共识协议的节点行为进行评价度量，将偏离共识协议的节点从共识系统中剔除，以保证协议在多数诚实节点上执行并达成一致性。

共识机制中主节点为集合形式的存在，一定通信量的产生使得改进的 PBFT 共识机制不会频繁更换视图。恶意节点会在共识机制的节点状态更新中被删除，相应信誉值较低的节点也会因为信誉机制的迭代从系统中被剔除。因此，共识节点中的节点可信度保证了共识一致性的达成。

5.2.3 活性

改进的 PBFT 共识算法的活性主要由 PBFT 共识过程中的视图切换和信誉机制的迭代提供。在共识节点组内或组间的共识过程中，通过均匀分布的随机性来选取信誉值良好的节点作为主节点，而共识视图编号依次递增。在共识节点收到超时信息或者主节点为恶意的情形下，若有 $f_{malicious}+1$ 个共识节点确认当前视图无效，则共识节点一致性地进入下一个视图进行共识协议的执行。

当主节点发生故障时，组内共识节点通过算法 1 进行主节点的选取更新，以保证改进的 PBFT 共识算法能够拥有应对节点宕机故障的能力，结合信誉机制的主节点选举则保证了主节点的可靠性，在降低主节点偏离协议的概率的同时增强了改进的 PBFT 共识算法的活性。

6 实验分析与讨论

6.1 功能性对比分析

现有结合信誉机制的共识方案中都存在不同程度的信誉积累问题，进而给系统的安全性带来了一定的威胁。表 4 列出了本文方案与其他方案在可扩展性、信誉积累程度、激励机制的存在性以及综合性能方面的对比结果。

表 4 各方案的功能性对比

Table 4 Performance comparison of different schemes

相关方案	可扩展性	信誉积累程度	激励机制	综合性能
文献[12-15]中的方案	高	高	无	中
文献[16]中的方案	中	高	有	中
文献[25]中的方案	中	中	有	中
本文方案	高	低	有	高

文献[12-15]与文献[16]中的信誉模型都有很高的信誉积累问题，虽然文献[25]中的信誉模型有较好的信誉机制，但其整体的性能适中，且需要可信第三方介入，使得模型的局限性较大。本文方案在解决信誉积累问题的基础上设计了激励机制来保证方案的稳健性。

6.2 共识机制性能对比分析

本节主要采用 python 语言对本文提出的共识算法与文献[15-16,25]中的信誉模型方案进行仿真对比。在 3.60GHz 的 8 核 64 位 Intel(R) Core(TM) i7-4790U 处理器、12GB 内存(RAM)、Windows10 操作系统的实验环境中，通过设置不同节点数量、在交易事务吞吐量、节点信誉值变化等方面对共识算法进行评测分析。同时对节点信誉演化模型进行仿真实验，实验结果证明本文设计的信誉机制的演化稳定有效。

6.2.1 吞吐量性能

实验将改进的 PBFT 算法中的共识节点依据信誉值进行分组，算法的最优性能分组依据节点的信誉值演化，首先设置共识节点在分组数目为 3、分组组内节点数目为 4、分组数目为 4、分组组内节点数目为 5 这 4 种不同情形下，对改进算法的吞吐量性能进行数值仿真，结果如图 8 所示。组内数目为 4 或 5 时，节点的并发度较稳定，吞吐量性能明显优于设置

分组数目为 3 或 4 的情形，而随着节点的增加，分组数目为定值时，组内的节点数目增多，导致改进的 PBFT 算法的吞吐量随着分组数的增加而下降，但此时信誉机制的存在仍使得改进算法的安全性比 PBFT 算法高。

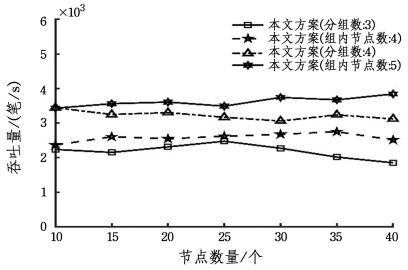


图 8 不同分组情形下的吞吐量性能

Fig. 8 Throughput performance in different packet scenarios

在本节的仿真实验中，通过设定不同节点数量在共识吞吐量性能方面对文献[15-16,25]以及本文提出的信誉机制方案进行测试，评测结果如图 9 所示。

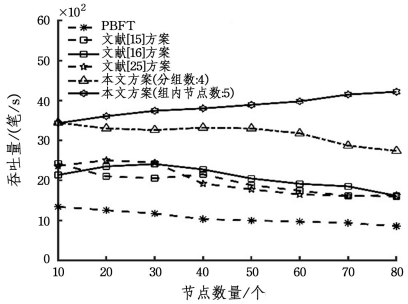


图 9 各方案吞吐量的对比

Fig. 9 Throughput comparison of different schemes

从仿真结果可以看出，在系统稳定时，节点数量的增加对改进的 PBFT 算法的吞吐量影响较小，而 PBFT 算法的吞吐量呈下降趋势。共识算法(含文献[15-16,25]和本文提出的算法)整体的吞吐量性能随着节点数量的增多而呈下降趋势。在节点数量设置为 40 及以上时，共识算法之间吞吐量的差值最为明显，其中 PBFT 共识算法的平均吞吐量为 956，改进的 PBFT 共识算法(分组数目为 4)的平均吞吐量达到 3081，而文献[15-16,25]中的方案最高的平均吞吐量为 2109。由此可见，改进的 PBFT 共识算法的平均吞吐量相比文献[15-16,25]中最高的平均吞吐量提升了 40%。

6.2.2 方案信誉模型对比

针对本文设计的信誉模型与文献[15-16,25]提出的信誉模型进行仿真对比。图 10 给出了同一共识节点在共识过程中不同信誉模型下信誉值的变化过程。

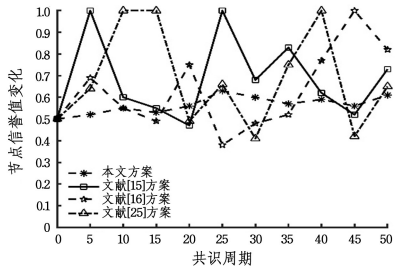


图 10 不同信誉模型下的节点信誉值变化

Fig. 10 Node reputation value under different reputation models

文献[15-16,25]都采用间断式的计算函数对节点进行赋值，使得在某一周期内，共识表现良好的节点会拥有较大的投票能力，导致方案趋于中心化，不利于方案的扩展。如图 10 所示，本文设计的信誉计算模型对同一共识节点在共识周期中有着平稳的信誉变化，即使在当选主节点时，也不会出现信誉的跳跃性变化，且所设计的基于信誉的激励机制对应的主节点与共识节点有不同的激励分配方式，保证了方案的稳健性。

6.2.3 改进的 PBFT 算法的共识成功率分析

在设置不同 $f_{malicious}$ 个数比率的情形下，对改进的 PBFT 共识算法的成功共识率与共识周期中共识节点的平均信誉值进行关联性仿真实验。设恶意节点的占比分别为 0.10，0.20，0.25，0.30，总节点的数目 $N=50$，同时配置不同类型的节点，如表 5 所列。在无激励机制的影响下，结果如图 11 所示。固定系统中 $f_{malicious}$ 的比率，随着系统平均信誉值的增加，系统趋于稳定状态且共识的成功率也逐渐趋于稳定。

表 5 策略阈值

Table 5 Thresholds of strategies

阈值区间	节点策略类型
(0.6,1.0]	诚实(honesty)
[0.4,0.6]	合作(cooperation)
[0,0.4)	背叛(betrayal)

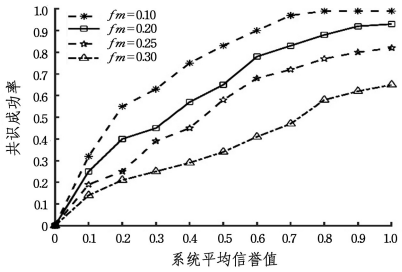


图 11 结合系统平均信誉值的共识成功率

Fig. 11 Consensus success rate combined with the average reputation value of the system

当恶意节点的占比为 0.25 时，在系统平均信誉阈值超过 0.6 后，共识的成功率逐渐趋于平缓，最终达到稳定值 0.82，此时系统中恶意节点的影响已被排除在共识系统之外，但共识成功效率仍然受到部分消极共识节点的影响[26]。当恶意节点的占比为 0.30 时，由于初始系统的平均信誉值较低，使得共识的成功率无法达到正常水平，但随着正常共识周期轮次的增加，使得正常共识节点的信誉值逐渐增加，但由于共识算法不能完全隔离恶意节点，使得系统中消极共识节点与恶意节点并存，导致共识成功率在系统稳定时仍处于较低的水平。但信誉机制的存在使得共识的成功率在可控容阈值内得到可观的平稳变化，使得陡增的恶意节点对系统瞬时的破坏性减小。

图 12 给出了在激励机制下，当恶意节点比率分别为 0.25 与 0.30 时，改进的 PBFT 算法共识成功率与系统平均信誉值的变化结果，其中 n-fm 表示无激励机制参与，fm 表示激励机制存在的情形。

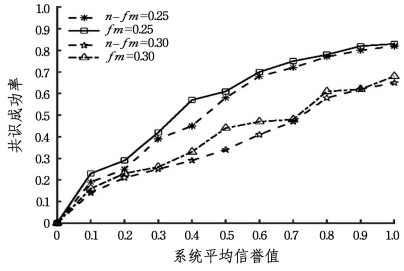


图 12 激励机制下的共识成功率

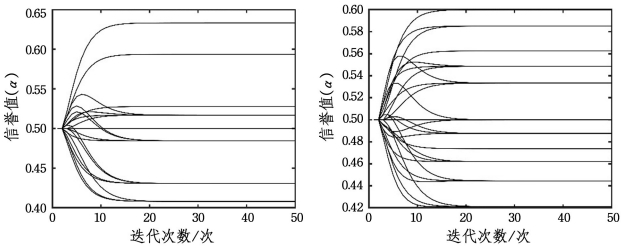
Fig. 12 Consensus success rate under the incentive mechanism

在加入激励机制的情形中，对消极共识节点的共识行为进行积极的促进，基于信誉演化策略的选择，理性的共识节点拥有良好的信誉值，对成功共识起到积极的作用。由图 12 可知，在激励机制的促进下，信誉值良好的节点对应更高的信誉收益，而共识过程中消极共识节点的共识积极性得到了提升，使得基于理性的信誉激励机制对达成共识起到重要的积极作用。

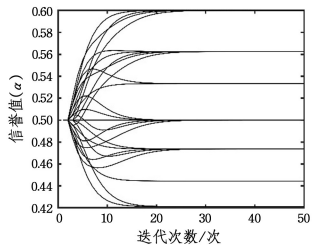
6.3 共识节点信誉机制的演化分析

针对本文设计的信誉机制采用 Matlab 语言进行仿真分析，主要通过模拟节点在共识机制信誉机制下的信誉演化过程，来分析共识节点信誉在链路中的变化。表 5 列出了仿真实验系统中的节点信誉策略阈值的设定，按照信誉值区间降序排序分别设定了合作、诚实、背叛 3 种行为策略集。

图 13 给出了不同节点信誉值演化收敛过程和信誉值演化过程。本节实验中，设定节点初始信誉值 $\alpha=0.5$，信誉迭代轮次 $t=5$，实验设定迭代周期轮次为 $T=50$，同时节点演化速率设定在[0.4,0.7]。



(a) $N=20$ 时，节点信誉值的收敛过程 (b) $N=30$ 时，节点信誉值的收敛过程



(c) $N=40$ 时，节点信誉值的收敛过程

图 13 演化模型中节点信誉值的收敛过程

Fig. 13 Convergence process of node reputation value in evolution model

由图 13 可知，节点信誉演化稳定状态都在设定的安全阈值之内，迭代次数稳定在 15～20 次之间可以达到收敛状态。本实验对节点到达信誉演化稳定的周期过程进行仿真，而受节点之间拓扑链接的变化影响，最终演化模型中节点的信誉值应该在最终收敛阈($\alpha^*-\varepsilon,\alpha^*+\varepsilon$)之内波动，而共识节点最终与链路状态达成一致，使得系统处于演化模型中的稳定状态。

设置的拓扑链路结构中的节点数目分别为 20,30,40，主要是对节点信誉值在激励机制中的动态变化进行模拟，从而得出演化稳定策略在不同节点数量的情况下的收敛性。仿真过程中对不同节点分配不同的演化速率，使得节点的信誉值不仅受到链路交互的影响，同时还受到系统环境因素的制约，这使得信誉值在演化模型中的变化更加具有可靠性。当节点数量为 20 时，共识节点信誉值在模型迭代 20 次左右达到收敛，收敛状态维持在[0.4,0.64]之间；而当节点数量设定为 30 时，节点信誉值仍然稳定在[0.42,0.6]之间。

结束语 结合信誉机制的容错算法中通常会因为机制原理产生信誉积累问题，使得采用算法的系统中心化程度较高，导致系统出现安全性问题，且不利于系统的扩展。基于此，本文提出了一种基于信誉和演化博弈模型的 PBFT 算法，在尝试解决原 PBFT 算法吞吐量等性能低的基础上，结合循环重置的信誉机制在保证安全的前提下解决信誉积累问题，并设计激励机制提升方案的稳健性。仿真测试表明，与同类算法相比，本文算法在吞吐量与信誉机制方面有着明显的优势，且信誉机制良好的收敛效果保证了系统共识的稳健性。

参 考 文 献

[1] CASTRO M,LISKOV B. Practical Byzantine Fault Tolerance [C]// Proceedings of the Third Symposium on Operating Systems Design and Implementation. New York: ACM Press, 1999: 173-186.

[2] SUKHWANI H, MARTÍNEZ J M, CHANG X L, et al. Performance Modeling of PBFT Consensus Process for Permissioned Blockchain Network (Hyperledger Fabric) [C]// 2017 IEEE 36th Symposium on Reliable Distributed Systems. NJ: IEEE Press, 2017: 253-255.

[3] GAO S, YU T Y, ZHU J M, et al. T-PBFT: An EigenTrust-based Practical Byzantine Fault Tolerance Consensus Algorithm [J]. China Communications, 2019, 16(12): 111-123.

[4] LI Y X, WANG Z, FAN J, et al. An Extensible Consensus Algorithm Based on PBFT [C]// 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery. NJ: IEEE Press, 2019: 17-23.

[5] NWEBONYI F N, MARTINS R, CORREIA M E. Reputation based Approach for Improved Fairness and Robustness in P2P Protocols[J]. Peer-to-Peer Networking and Applications, 2019, 12(4): 951-968.

[6] GAYVORONSKAYA T M. Blockchain: Hype Or Innovation [M]// Springer International Publishing AG. Berlin: Springer, 2021: 1-14.

[7] BOU A J, EI S R, KAMBHAMPATY K, et al. Permissionless Reputation-based Consensus Algorithm for Blockchain [J]. Internet Technology Letters, 2020, 3(3): 7-12.

[8] ZHU S C, ZHANG Z Y, CHEN L Q, et al. A PBFT Consensus Scheme with Reputation Value Voting based on Dynamic Clustering[C]// International Conference on Security and Privacy in Digital Economy. Singapore: Springer, 2020: 336-354.

[9] LIU Z Y, LUONG N C, WANG W B, et al. A Survey on Blockchain: A Game Theoretical Perspective[J]. IEEE Access, 2019, 7(4): 47615-47643.

[10] LI W Y, FENG C L, ZHANG L, et al. A Scalable Multi-layer PBFT Consensus for Blockchain[J]. IEEE Transactions on Parallel and Distributed Systems, 2020, 32(5): 1146-1160.

[11] XU X L, ZHU D W, YANG X X, et al. Concurrent Practical Byzantine Fault Tolerance for Integration of Blockchain and Supply Chain[J]. ACM Transactions on Internet Technology, 2021, 21(1): 1-17.

[12] LEI K, ZHANG Q C, XU L M, et al. Reputation-based Byzantine Fault Tolerance for Consortium Block-chain[C]// 2018 IEEE 24th International Conference on Parallel and Distributed Systems. NJ: IEEE Press, 2018: 604-611.

[13] BIRYUKOV A, FEHER D. ReCon: Sybil-resistant Consensus from Reputation[J]. Pervasive and Mobile Computing, 2020, 61(1): 1-29.

[14] CHEN P, HAN D Z, WENG T H, et al. A Novel Byzantine Fault Tolerance Consensus for Green IoT with Intelligence based on Reinforcement[J]. Journal of Information Security and Applications, 2021, 59(6): 131-139.

[15] LIA Y X, BO Z X, LIU J. Research on Sybil Attack in Defense Blockchain based on Improved PBFT Algorithm[J]. Journal on Communications, 2020, 41(9): 104-117.

[16] YU J S, KOZHAYA D, DECOUCHANT J, et al. Repucoin: Your Reputation is Your Power[J]. IEEE Transactions on Computers, 2019, 68(8): 1225-1237.

[17] BOU A J, EI S R, DEMERJIAN J. Permissionless Proof-of-Reputation-X: A Hybrid Reputation-based Consensus Algorithm for Permissionless Blockchains[J]. Transactions on Emerging Telecommunications Technologies, 2021, 32(1): 383-410.

[18] MANSHAEI M H, JADLIWALA M, MAITI A, et al. A Game-Theoretic Analysis of Shard-based Permissionless Blockchains [J]. IEEE Access, 2018, 6(12): 78100-78112.

[19] TIAN Y L, PENG C G, MA J F, et al. Game-Theoretic Mechanism for Cryptographic Protocol[J]. Journal of Computer Research and Development, 2014, 51(2): 344-352.

[20] DING H F, PENG C G, TIAN Y L, et al. Privacy Risk Adaptive Access Control Model via Evolutionary Game[J]. Journal on Communications, 2019, 40(12): 9-20.

[21] SANDHOLM W H. Population Games and Evolutionary Dynamics[M]// Massachusetts Institute of Technology MIT Press. London: The MIT Press, 2010: 119-140.

[22] LI S J, SU W L. The Research of Reputation Incentive Mechanism of P2P Network File Sharing System[J]. International Journal of Information and Computer Security, 2018, 10(2/3): 149-169.

[23] RANJBAR-SAHRAEI B, BOU A H, BLOEMBERGEN D, et al. Evolution of Cooperation in Arbitrary Complex Networks [C]// Proceedings of the 2014 International Conference on Autonomous Agents and Multi-agent Systems. New York: ACM Press, 2014: 677-684.

[24] HARTMAN P. A Lemma in The Theory of Structural Stability of Differential Equations[J]. Proceedings of the American Mathematical Society, 1960, 11(4): 610-620.

[25] WANG E K, LIANG Z D, CHEN C M, et al. PoRX: A Reputation Incentive Scheme for Blockchain Consensus of IioT[J]. Future Generation Computer Systems, 2020, 102(1): 140-151.

[26] MALKHI D, NAYAK K, REN L. Flexible Byzantine Fault Tolerance[C]// Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2019: 1041-1053.

YANG Xin-yu, born in 1998, master student. His main research interests include consensus mechanism and game theory.

DING Hong-fa, born in 1988, Ph.D, associate professor. His main research interests include privacy protection and data security.

（责任编辑：柯颖）