计算机科学
COMPUTER SCIENCE

# BDBFT:一种物联网场景下基于信誉预测模型的共识协议

王璞, 高湛云, 王振飞, 宋哲理

引用本文

王璞, 高湛云, 王振飞, 宋哲理. BDBFT:一种物联网场景下基于信誉预测模型的共识协议[J]. 计算机科学, 2025, 52(5): 366-374.

WANG Pu, GAO Zhanyun, WANG Zhenfei, SONG Zheli. BDBFT:A Consensus Protocol Based on Reputation Prediction Model for IoT Scenario [J]. Computer Science, 2025, 52(5): 366-374.

---

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.240300018

# BDBFT:一种物联网场景下基于信誉预测模型的共识协议

王 璞[1] 高湛云[1] 王振飞[1] 宋哲理[2]
1 郑州大学计算机与人工智能学院 郑州 450001
2 郑州财税金融职业学院信息技术系 郑州 450048
(iezfwang@zzu.edu.cn)

**摘 要** 区块链技术在物联网场景的应用中具有强数据安全性和高可信度的优势,但区块链技术中的共识算法存在能耗高、计算成本高、可扩展性低等缺点,在物联网应用中部署区块链系统面临物联网节点存储容量小、能耗低和计算能力不足的问题。在实用拜占庭容错算法(PBFT)的基础上,提出了一种物联网场景下基于信誉预测模型的共识协议(BDBFT)。首先,根据分组策略的地理位置分类标准对节点进行分组以选取共识节点,减少组内通信的通信时延;其次,引入基于 Dirichlet 分布的细粒度信誉预测模型,根据每轮视图生命周期中的信誉信息动态地更新模型,并基于历史信誉信息和当前信誉信息投票高预测概率的节点作为共识节点。仿真实验结果表明,相对于 PBFT 算法和 LRBFT 算法,BDBFT 算法有效地降低了拜占庭节点参与共识的概率,在时间延迟、吞吐量、通信开销和安全性 4 个方面具有明显的性能提升。

**关键词**:物联网;区块链;PBFT;Dirichlet 分布;分组策略;信誉预测模型
**中图分类号** TP311

# BDBFT:A Consensus Protocol Based on Reputation Prediction Model for IoT Scenario

WANG Pu[1],GAO Zhanyun[1],WANG Zhenfei[1] and SONG Zheli[2]
1 College of Computer and Artificial Intelligence,Zhengzhou University,Zhengzhou 450001,China
2 Department of Information Technology,Zhengzhou Vocational College of Finance and Taxation,Zhengzhou 450048,China

**Abstract** Blockchain technology has the advantages of strong data security and high trustworthiness in IoT scenarios,but the consensus algorithm in blockchain technology has the disadvantages of high energy consumption,high computational cost,and low scalability,and the deployment of blockchain system in IoT applications faces the problems of low storage capacity,low energy consumption,and low computational capacity of IoT nodes. Based on practical Byzantine fault tolerant algorithm(PBFT),this paper proposes a consensus protocol based on reputation prediction model(BDBFT) in IoT scenario. Firstly,nodes are grouped according to the geographic location classification criteria of the grouping policy to select consensus nodes and reduce the communication delay of intra-group communication. Secondly,a fine-grained reputation prediction model based on Dirichlet distribution is introduced to dynamically update the model according to the reputation information in the lifecycle of each round of view,and nodes with high prediction probability based on the historical and current reputation information are voted as the consensus nodes. The simulation experiment results show that compared with PBFT algorithm and LRBFT algorithm,BDBFT algorithm effectively reduces the probability of Byzantine nodes participating in the consensus,and has obvious performance improvement in four aspects:time delay,throughput,communication overhead and security.

**Keywords** IoT,Blockchain,PBFT,Dirichlet distribution,Grouping strategy,Reputation prediction model

## 1 引言

物联网(IoT)是一个由众多相互连接的物体、服务、人类和设备构成的庞大网络系统。物联网通过互联互通,实现数据通信、信息共享和交互合作,旨在提高生产效率、优化资源利用、提供更好的用户体验,并在各个领域创造新的商业和服务机会,如智能家居、汽车、农业、医疗、能源生产等多个领域。然而,随着物联网设备数量的激增,传统的物联网应用面临大规模的设备管理,数据完整性、可靠性等诸多挑战[1]。

区块链本质上是一个多节点共同维护的具有去中心化、防篡改、可编程和可追溯等特点的分布式数据库[2]。区块链技术为物联网存在的数据安全问题提供了新的解决方案,如

到稿日期:2024-03-02 返修日期:2024-07-19
基金项目:国家重点研发计划(2023YFB4502704);河南省科技攻关项目(232102210189)
This work was supported by the National Key Research and Development Program of China(2023YFB4502704) and Science and Technology Research Project of Henan Province(232102210189).
通信作者:宋哲理(710491238@qq.com)

今物联网-区块链应用受到各个领域的青睐[3]，如工业[4]、能源[5]、自动驾驶[6]、医疗保健[7]等。共识算法作为区块链的核心机制，是保障网络中的多个节点对于数据的状态和顺序达成共同决策的算法[8]。区块链共识算法主要分为证明类共识算法（如 PoW[9]，PoS[10]，DPoS[11]等）和拜占庭共识算法（如 PBFT[12]等）。目前大多数物联网-区块链应用采用 PoW 算法作为其共识算法。PoW 算法中所有节点需要通过解决一个复杂的数学问题，即所谓的工作量，来竞争获得创建新区块的权利，解决问题最快的节点利用获得的权力生成一个新的块并获得一定数量的虚拟货币奖励。然而，由于节点在竞争新区块的出块权力时需要进行大量的计算工作，因此会造成大量能源的浪费；其次，如果少数矿工掌握大部分算力，则会严重影响区块链网络的安全性和去中心化。在物联网场景下，物联网设备通常具有有限的计算资源和电池寿命，难以支持 PoW 算法高能耗的计算过程，相对于 PoW 算法，PBFT 算法在确保区块链系统安全性和拜占庭容错方面具有高吞吐量、低能耗和高容错的优势，更适用于物联网-区块链应用。但是，PBFT 算法仍存在许多问题亟待改进。首先，PBFT 算法的时间复杂度为 $O(n^2)$，高昂的通信代价造成其在大规模网络中的低可扩展性和高通信时延的问题；其次，PBFT 算法主节点选取机制随意且简单，所有节点均为共识节点，主节点按顺序选取，这可能带来单点故障、恶意操控、视图频繁切换等问题；最后，PBFT 算法缺少共识节点的评估机制，系统的安全性无法得到保障。

针对上述 PBFT 算法可扩展性差、主节点选取简单、缺少共识节点评估机制的问题，本文提出了适用于物联网场景下改进的拜占庭容错算法（BDBFT）。BDBFT 算法引入基于 Dirichlet 分布的细粒度信誉预测模型和分组策略，通过信誉预测模型，降低拜占庭节点参加共识决策的概率；同时通过分组策略将大规模网络节点进行划分，同时允许节点动态地加入区块链网络，有效减小系统的通信代价。分析表明，BDBFT 算法有效减小了系统开销，同时提高了系统的鲁棒性和可扩展性，可以为物联网-区块链应用提供高可用性的支持。

## 2　相关工作

现阶段国内外研究者提出了许多关于 PBFT 共识算法的改进方案。DBFT[13]算法是一种委托式拜占庭容错共识算法，结合 PoS 算法的思想，通过投票机制推选部分节点负责验证交易和出块的工作，然而该算法采用代理记账节点，在节点数量有限时可能导致中心化风险，使得安全性降低。多层可扩展 PBFT 算法[14]通过将节点分成不同的层次并限制组内通信来实现更好的性能，然而分层的层数是对算法性能权衡的一个挑战。文献[15]提出了一种结合 PoS 算法和 PBFT 算法的共识机制，通过信任分数和奖励机制作为区块验证和排序过程中的重要组成部分以激励节点诚实行为，并通过半马尔可夫过程分析模型验证共识机制的有效性。ABC-GSPBFT[16]算法将分组评分机制和人工蜂群算法相结合，通过人工蜂群算法预选可靠节点集合，并通过分组评分机制再次选取共识节点，大幅度降低了共识节点的规模，并保证了节点的可靠性。LRBFT[17]算法使用拉格朗日插值法生成随机种子，优化主节点集选举过程的随机性，通过委托节点减少共识节点规模，从而提高共识效率。BW-PBFT[18]算法通过引入基于信誉值双向衰减机制和层次分析过程来评估节点质量，并结合投票和信誉值的选取机制组建委员会，使高可靠性的节点有更高的几率参与区块共识过程。E-PBFT[19]采用节点间随机匹配的通信方式替换节点全广播的通信方式，成功降低了节点间的通信次数。DT-PBFT[20]赋予节点属性，将属性作为参数输入到信誉计算算法中，根据信誉计算结果选择双层共识模型中的主节点。

从区块链-物联网应用的角度来看，国内外学者主要根据应用场景差异改进 PBFT 算法架构。R-PBFT[21]算法在车联网场景中引入逻辑回归计算的声誉机制，根据节点的声誉值划分角色，在提高安全性的同时减小了验证和记录交易的开销。P-PBFT[22]算法结合药品供应链的特点，通过响应速度将大规模网络节点划分为不同的共识集进行分组共识，实现药品溯源系统更小的延迟和更高的吞吐量。SG-PBFT[23]算法是适用于车联网的安全高效共识算法，通过分组机制改进传统 PBFT，降低中心服务器压力，提高共识效率，并抵御单节点攻击。SBFT[24]使用收集器汇总消息，结合节点贡献值和可验证随机函数改进主节点选取方法，保证主节点选取的安全性和不可预测性。

综上所述，现有的对于 PBFT 共识算法的研究分为两个方面：1）通过门限签名或节点角色划分减少共识节点规模；2）通过引入信誉值评估方法或改进随机选举方案来减少恶意节点参与共识的概率。但它们的信誉值评估方法相对简单，且缺乏适用于在物联网-区块链场景下结合地理位置信息和信誉预测模型的 PBFT 共识算法的研究。

## 3　相关知识

在详细介绍 BDBFT 算法之前，本章将介绍 PBFT 共识算法和 Dirichlet 分布的相关知识。

### 3.1　PBFT 共识算法

实用拜占庭容错（Practical Byzantine Fault Tolerance，PBFT）是拜占庭容错算法的一种实用型改进算法，用于处理完全不可信的分布式系统环境中的拜占庭将军问题，它成功地将消息一致性协议的时间复杂度从指数级降低到多项式水平。PBFT 算法描述的节点有 3 个角色：主节点、副本节点和客户端。客户端生成和打包交易并发送给主节点和副本节点，主节点和副本节点执行一致性协议达成共识。如果区块链网络中节点总数为 $N$，PBFT 算法可以容忍的拜占庭节点数量为 $F\leqslant\frac{N-1}{3}$，当区块链网络中拜占庭节点数量满足不等式，则 PBFT 算法可以通过备份节点和主节点之间的信息交换达成共识。PBFT 算法的流程如图 1 所示。PBFT 算法的一致性算法描述如下。

1）REQUEST 阶段：客户端 $c$ 生成事务请求，向主节点发送请求消息 $\langle REQUEST,o,t,c\rangle\sigma_c$。其中，$o$ 表示客户端发起的具体操作，$t$ 表示消息生成的时间戳，$\sigma_c$ 是客户端对消息的签名。

2）PRE-PREPARE 阶段：主节点 $p$ 验证请求消息的真实

性，在当前视图 $v$ 下对该消息分配唯一的消息序列号 $n$，广播预准备消息〈〈*PRE-PREPARE*，$v$，$n$，$d$〉$\sigma_p$，$m$〉给所有副本节点。其中，$m$ 是主节点捎带的消息，$d$ 是 $m$ 的消息摘要，$\sigma_p$ 是主节点对消息的签名。

3）PREPARE 阶段：副本节点 $i$ 验证消息内容和主节点签名，向其他节点广播准备消息〈*PREPARE*，$v$，$n$，$d$，$i$〉$\sigma_i$，告知其他节点自己已经收到这个事务请求。其中，$\sigma_i$ 是副本节点 $i$ 对消息的签名。

4）COMMIT 阶段：若副本节点 $i$ 收到来自其他节点的正确准备消息数量达到 $2f$，则执行消息中的事务请求，并向其他节点广播提交消息〈*COMMIT*，$v$，$n$，$d$，$i$〉$\sigma_i$，通知其他节点该事务请求已经得到执行。

5）REPLY 阶段：当副本节点 $i$ 收到来自 $2f+1$ 个不同节点的提交消息，将共识完成的时间戳 $t$ 和共识执行结果 $r$ 打包到回复消息〈*REPLY*，$v$，$t$，$c$，$i$，$r$〉$\sigma_i$ 中，最后向客户端 $c$ 发送回复消息，通知其事务请求已完成并达成共识。当客户端 $c$ 收到来自 $f+1$ 个不同节点的回复消息时，确信最初发送的事务请求已经达成共识。

当 PBFT 算法在面临主节点发生故障、发生不诚实行为和被副本节点检测为故障节点而导致共识无法达成的场景时，将会触发视图切换协议，即选取其他诚实节点作为主节点以继续引导共识过程。PBFT 算法的视图切换协议可以保证区块链系统的安全性和活性。

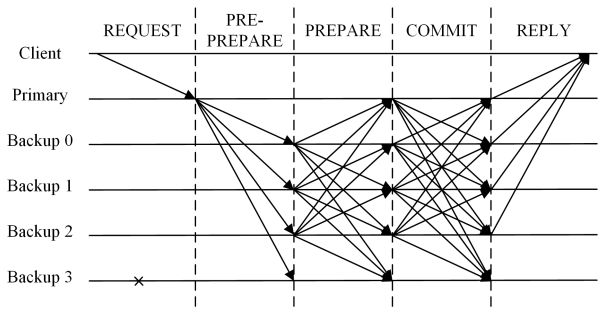


图 1 PBFT 算法的流程

Fig. 1 Workflow of PBFT algorithm

### 3.2 Dirichlet 分布

提出的信誉预测模型是基于贝叶斯理论中的 Dirichlet 分布实现的。基于 Dirichlet 分布构建的信誉预测模型，将节点的信誉划分为若干等级，模型根据节点获得的信誉等级计数向量动态地更新对其他节点预测的信誉概率。

Dirichlet 分布是多项分布的共轭先验分布，它是一个多维概率分布，用于描述在多项分布中每个事件概率参数的不确定性。Dirichlet 分布提供多项分布概率参数的先验分布，允许在观测到数据后更新概率参数的分布。假设有多个同分布的随机变量序列 $U_1$，$U_2$，$U_3$，…，它们取 $k$ 个结果中的一个，结果集表示为 $\{o_i\}_{i=1}^{k}$。假设 $p_i=Pr(U_j=o_i)(1\leqslant i\leqslant k)$ 表示随机变量的概率密度，概率的向量表示为 $\vec{p}=(p_1,p_2,\cdots,p_k)$，其中 $p_i>0$ 且 $\sum_{i=1}^{k}p_i=1$。

假设 $\vec{p}=(p_1,p_2,\cdots,p_k)$ 具有 Dirichlet 分布的共轭先验分布，则每一个 $p_i$ 对应一个 $\alpha_i$ 作为其先验观测计数，先验观测计数向量表示为 $\vec{\alpha}=(\alpha_1,\alpha_2,\cdots,\alpha_k)$。Dirichlet 分布的概率密度函数如式(1)所示：

$$f(\vec{p}\mid\vec{\alpha})=Dir(\vec{p}\mid\vec{\alpha})=\frac{\Gamma(\sum_{i=1}^{n}\alpha_i)}{\prod_{i=1}^{n}\Gamma(\alpha_i)}\prod_{i=1}^{n}p_i^{\alpha_i-1} \tag{1}$$

其中，$\Gamma$ 是伽马函数。Dirichlet 分布作为一种常用的贝叶斯推理方法，具有先验分布和后验分布共轭的特点，即后验分布与先验分布都服从 Dirichlet 分布。假设后验观测计数向量为 $\vec{\beta}=(\beta_1,\beta_2,\cdots\beta_k)$，则后验分布的概率密度函数如式(2)所示：

$$\begin{aligned}f(\vec{p}\mid\vec{\alpha}+\vec{\beta})&=\frac{f(\vec{\alpha}+\vec{\beta}\mid\vec{p})\times f(\vec{p})}{f(\vec{\alpha}+\vec{\beta})}\\&=Dir(\vec{p}\mid\alpha_1+\beta_1,\alpha_2+\beta_2,\cdots,\alpha_k+\beta_k)\end{aligned} \tag{2}$$

Dirichlet 分布的后验分布用于表述概率 $p_i$ 的更新。$p_i$ 的后验均值则用于表示在未来实验中观测到结果为 $\sigma_i$ 的概率，$p_i$ 的后验均值如式(3)所示：

$$E[p_i\mid\vec{\alpha}+\vec{\beta}]=\frac{\alpha_i+\beta_i}{\sum_{i=1}^{k}(\alpha_i+\beta_i)} \tag{3}$$

## 4 BDBFT 共识算法

### 4.1 信誉预测模型

BDBFT 算法设计基于 Dirichlet 分布的细粒度信誉预测模型，用于有效识别复杂的区块链网络中的恶意节点。所有节点在本地部署信誉预测模型，在每轮共识中评估其他节点的信誉等级。但是考虑到节点自身所获取的信誉信息具有局限性，不能合理地对节点进行评估，因此不仅需要考虑节点的当前信誉信息，信誉评估模型还要参考节点的历史信誉信息。为方便对 BDBFT 算法的信誉预测模型进行描述，在下文中假定以 $k$ 视图下节点 $N_a$ 评估节点 $N_b$ 的信誉信息为例，相关概念的定义如下。

**定义 1**（信誉值） 信誉值是用于衡量一个节点在网络中的可信程度和可靠性的定量指标，通常是基于节点在过去的行为、表现和交互中所展现的特征和属性进行计算得出的。提出的信誉预测模型中，对节点的信誉值评估需要从时间和空间两个维度进行分析。在 $k$ 视图下，对 $m$ 区块进行共识的过程中，$D_{a,b}(m)$ 和 $G_{a,b}(m)$ 表示节点 $N_a$ 对节点 $N_b$ 从时间维度和空间维度量化计算获得的延迟指数和空间指数，并赋予不同的权重参数 $\delta$ 和 $1-\delta$，取值范围在 0～1。节点 $N_a$ 评估节点 $N_b$ 信誉值 $T_{a,b}^{k,m}$ 的计算方法如式(4)所示：

$$T_{a,b}^{k,m}=\delta D_{a,b}(m)+(1-\delta)G_{a,b}(m) \tag{4}$$

**定义 2**（信誉等级） 信誉评估模型将节点共识行为的信誉划分为 $n$ 个等级，第 $i$ 个信誉等级用 $l_i$ 表示，其中 $i=1,2,\cdots,n$，$i$ 越大，信誉等级越高。若 $T_{a,b}^{k,m}$ 的取值为 $\left(\frac{i-1}{n},\frac{i}{n}\right)$，则认为在第 $k$ 个视图下，对第 $m$ 个区块共识行为的信誉等级为 $l_i$。

**定义 3**（信誉等级计数向量） 信誉等级计数向量表示视图中节点 $N_a$ 对其他节点共识行为的评估结果为信誉等级 $l_i$ 的计数向量。在第 $k$ 个视图下，$\alpha_{a,b}^{k,i}$ 用于表示节点 $N_a$ 评估节点 $N_b$ 当前行为的信誉等级为 $l_i$ 的计数器，其中 $0\leqslant i\leqslant n$，则信誉

等级计数向量如式(5)所示：

$$\overrightarrow{A_{a,b}^{k\_l}}=\{\alpha_{a,b}^{k\_1},\alpha_{a,b}^{k\_2},\cdots,\alpha_{a,b}^{k\_n}\} \tag{5}$$

4.1.1　当前视图的信誉信息

当前视图的信誉信息是节点在当前视图下所有共识过程中所获得的对其他节点共识行为量化评估的信誉等级计数向量集合。在视图的生命周期中，节点记录的当前视图信誉等级计数向量的初始值为零向量，在每个区块的共识过程中，节点通过本地部署的基于 Dirichlet 分布的信誉预测模型，对节点行为进行监督和评估，依次计算信誉值和信誉等级，根据获得信誉等级的次数动态更新当前视图的信誉等级计数向量。如定义 1 所示，信誉值从时间和空间两个维度进行评估，信誉值计算的主要内容如下。

1)时间维度。在共识过程中，节点正常工作的稳定性是保证共识时间一致性的重要指标。通常情况下，如果拜占庭节点通过提供不稳定的计算能力、生成假消息、篡改消息等行为干扰共识流程，与正常节点的共识行为相比，它作恶所需的时间延迟要大得多。为综合考虑节点是否正常工作，从时间维度考虑，节点$N_a$需要评估节点$N_b$在第 $m$ 个区块共识过程的延迟指数，延迟指数的计算方法如式(6)所示：

$$D_{a,b}(m)=1-\left|\frac{t_r-t_q-\Delta t_e}{\widetilde{t_s}}\right| \tag{6}$$

其中，$t_r$和$t_q$分别是节点完成共识的时间和开始共识的时间，$\Delta t_e$是节点完成共识周期的平均时间，$\widetilde{t_s}$是系统预设的共识过程的最长等待时间。

2)空间维度。在物联网-区块链应用中，存在大量的固定物联网设备，例如智能城市中的路灯、传感器等，这些设备通常安装在固定的位置。选取地理位置固定的物联网节点作为共识节点，意味着节点之间的通信路径相对稳定，缩短了节点之间的消息传输时间和计算时间，从而减少了共识延迟，提高了系统的响应速度以及共识效率。BDBFT 使用 GeoHash 算法计算物联网节点的地理位置信息，节点$N_i$的地理位置哈希信息用字母$Gh(i)$表示。在共识过程中，节点需要在消息中加入地理位置哈希值，方便其他节点监督该节点的地理位置信息。因此，从空间维度考虑，节点$N_a$评估节点$N_b$在第 $m$ 个区块共识过程的空间指数的计算方法如式(7)所示：

$$G_{a,b}(m)=\begin{cases}0, & Gh(m-1)=Gh(m)\\ 1, & Gh(m-1)\neq Gh(m)\end{cases} \tag{7}$$

根据定义 1，节点$N_a$可以参考时间维度和空间维度信息，计算节点$N_b$的信誉值$T_{a,b}^{k_m}$；信誉值$T_{a,b}^{k_m}$通过定义 2 的映射关系获得相应的信誉等级$l_i$。信誉信息为了更好地惩罚节点作恶行为，提高系统的安全性，在信誉信息更新的过程中赋予低信誉等级更高的调谐参数$\frac{n+1-l}{3n}$，其中 $l$ 表示共识行为的信誉等级数。从调谐参数可以直观地看出，信誉等级越高，调谐参数越小，因此可以根据式(8)对定义 3 的信誉等级计数向量中对应的信誉等级计数器$a_{a,b}^{k_l}$进行更新。

$$\alpha_{a,b}^{k\_l}=\alpha_{a,b}^{k\_l}+\frac{n+1-l}{3n} \tag{8}$$

当第 $k$ 个视图的生命周期结束或需要执行视图切换机制时，节点$N_a$在 $k$ 视图评估节点$N_b$的每次共识行为，可以得到该视图下的信誉信息，即信誉等级计数向量$\overrightarrow{A_{a,b}^{kl}}$。

4.1.2　历史信誉信息

历史信誉信息为历史视图的信誉等级计数向量的总和。假设当前场景为 $k$ 视图，节点$N_a$评估节点$N_b$的历史信誉等级计数向量的计算方法如式(9)所示：

$$\begin{aligned}\overrightarrow{B_{a,b}^{k\_l}}&=\sum_{i=1}^{k-1}\overrightarrow{A_{a,b}^{i\_l}}\\&=\{\sum_{i=1}^{k-1}\alpha_{a,b}^{i\_1},\sum_{i=1}^{k-1}\alpha_{a,b}^{i\_2},\cdots,\sum_{i=1}^{k-1}\alpha_{a,b}^{i\_n}\}\\&=\{\beta_{a,b}^{k\_1},\beta_{a,b}^{k\_2},\cdots,\beta_{a,b}^{k\_n}\}\end{aligned} \tag{9}$$

4.1.3　节点预测概率计算

信誉预测模型基于 Dirichlet 分布实现，可以通过不断地更新观测计数，动态地更新节点为诚实节点概率。假定当前为 $k$ 视图生命周期结束，BDBFT 算法需要执行视图切换协议重新选举共识节点和主节点，在 $k$ 视图获得的当前视图的信誉等级计数向量可以理解为后验知识，而历史信誉等级计数向量之和可以理解为先验知识，通过后验知识更新信誉预测模型，进而计算更新后的节点预测概率。本节以节点$N_a$通过信誉预测模型计算节点$N_b$为诚实节点的预测概率为例。节点结合当前视图的信誉信息$\overrightarrow{A_{a,b}^{k_l}}$和历史信誉信息$\overrightarrow{B_{a,b}^{k_l}}$，可以得到更新后的概率密度函数，如式(10)所示：

$$\begin{aligned}&f(\vec{p}\mid\overrightarrow{B_{a,b}^{k\_l}}+\overrightarrow{A_{a,b}^{k\_l}})\\&=Dir(\vec{p}\mid\overrightarrow{B_{a,b}^{k\_l}}+\overrightarrow{A_{a,b}^{k\_l}})\\&=\frac{\Gamma(\sum_{i=1}^{n}\beta_{a,b}^{k\_i}+\alpha_{a,b}^{k\_i})}{\prod_{i=1}^{n}\Gamma(\beta_{a,b}^{k\_i}+\alpha_{a,b}^{k\_i})}\prod_{i=1}^{n}p_i^{\beta_{a,b}^{k\_i}+\alpha_{a,b}^{k\_i}-1}\end{aligned} \tag{10}$$

进一步可以得到节点$N_a$预测节点$N_b$信誉等级为$l_i$的期望，如式(11)所示：

$$E[p_i\mid\overrightarrow{B_{a,b}^{k\_l}}+\overrightarrow{A_{a,b}^{k\_l}}]=\frac{\beta_{a,b}^{k\_i}+\alpha_{a,b}^{k\_l}}{\sum_{i=1}^{k}(\beta_{a,b}^{k\_i}+\alpha_{a,b}^{k\_l})} \tag{11}$$

BDBFT 算法根据节点的分类采用不同的阈值 $\varphi$ 来计算预测概率。共识节点作为共识组成员节点，如果作恶将严重危害系统的安全和稳定性，因此设置阈值为 0.3；为提高副本节点被选举为共识节点的概率，鼓励其积极参与共识，因此设置高阈值为 0.5。这样的阈值设计有助于促进各类节点共同参与共识，提高系统的包容性和公平性。阈值 $\varphi$ 的选择可以根据具体应用场景和系统需求进行合理调整和优化，并根据充分的数据收集和信誉评估来确保准确性和公正性，为物联网-区块链应用提供稳健的共识机制。阈值 $\varphi$ 的设置如表 1 所列。节点$N_a$计算节点$N_b$的预测概率的计算式为：

$$P_{\text{pred}}=\begin{cases}\sum_{i=1}^{\lceil\varphi n\rceil-1}E[p_i\mid\overrightarrow{B_{a,b}^{k\_i}}], & 0\leqslant i<\lceil\varphi n\rceil\\ \sum_{i=\lceil\varphi n\rceil}^{n}E[p_i\mid\overrightarrow{B_{a,b}^{k\_i}}], & \lceil\varphi n\rceil\leqslant i\leqslant n\end{cases} \tag{12}$$

其中，$P_{\text{pred}}$表示节点$N_b$为恶意或诚实节点的概率。

表 1　阈值参数

Table 1　Threshold parameter

| 节点类型 | $\varphi$ | $1-\varphi$ |
|---|---|---|
| 共识节点 | 0.3 | 0.7 |
| 副本节点 | 0.5 | 0.5 |

4.1.4 正确性证明

采用数学归纳法验证信誉预测模型的正确性。信誉预测模型是 $n$ 维 Dirichlet 分布，即 $Dir(1,2,\cdots,n)$，节点初始的信誉等级计数向量为单位向量，$P_T$ 表示节点为诚实节点的概率，其值为 0.5。假设节点 $N_a$ 为评估节点，$N_b$ 为拜占庭节点，$N_b$ 的共识行为总是被评估为前 $\lceil \varphi n \rceil$ 个信誉等级，即获得的信誉等级计数向量 $\{\alpha_1,\cdots,\alpha_{\lceil \varphi n \rceil},0,\cdots,0\}$，其中 $\alpha_i=\frac{n+1-i}{3n}$，$i\in[1,n]$。为了方便进行验证，设置 $\varphi=0.5$。验证 $m$ 个视图周期后，$N_b$ 为诚实节点的概率 $P_T$ 始终在降低。

当 $m=1$ 时，$N_a$ 对 $N_b$ 评估的信誉等级计数向量为 $\left\{\frac{n}{3n},\cdots,\frac{n+1-\lceil \varphi n \rceil}{3n},0,\cdots,0\right\}$ 与历史信誉等级计数向量 $\{1,\cdots,1\}$ 结合，可以计算出 $N_b$ 未来行为被评估为信誉等级 $l_i$ 的概率 $p_i=\frac{\alpha_i+1}{\sum_{i=1}^{n}\alpha_i+n}$，$i\in[1,n]$，$P_T$ 的计算结果则为 $\sum_{i=\lceil \varphi n \rceil+1}^{n} p_i$。由获得的信誉等级计数向量可得，当 $\lceil \varphi n \rceil+1\leqslant i\leqslant n$ 时，$\alpha_i$ 的值为 0，$p_i$ 的分子为 1，分母变大，其值变小，因此 $P_T$ 的计算结果也会相较于未获得信誉等级计数向量之前更低，即 $P_T<0.5$。

当 $m=k$ 时，$N_a$ 对 $N_b$ 评估的信誉等级计数向量叠加，表示为 $\{k\alpha_1,\cdots,k\alpha_{\lceil \varphi n \rceil},0,\cdots,0\}$，对于 $P_T$ 的计算结果，分子始终不变，由于不断获得信誉等级计数向量，分母的值一直在增加，即 $P_T$ 的值一直在减小。

对于 $m=k+1$ 的情况，随着获得的信誉等级计数向量的增加，易证 $P_T$ 的值仍然在减小，故证明成立，即拜占庭节点在参与共识过程中，由于其作恶行为始终被评估为低信誉等级，在信誉预测模型的计算中，预测拜占庭节点为诚实节点的概率始终会降低。

### 4.2 分组策略

BDBFT 算法将节点划分为共识组和副本组，共识组需要根据时间顺序将多个交易打包成区块并对区块达成共识，副本组负责执行共识结果。在实际的物联网-区块链应用中，物联网节点之间距离的远近会对系统的通信时延、数据同步效率、能源开销、网络稳定性等造成影响，且实际生活中大部分物联网节点的地理位置基本是固定的。基于此，BDBFT 算法采用 GeoHash 算法计算节点的地理位置信息，且根据地理位置信息将节点划分为多个副本组，副本组通过随机选取机制选取共识节点作为副本组的领导者；共识节点通过信誉预测模型和主节点选取机制选择主节点。

4.2.1 分组初始化

如图 2 所示，分布在不同地理位置的物联网节点，如智能家居、车辆、手机、路由器、智能手表等，通过以太网连接在一起，每个节点在加入联盟时都已获得联盟链网络的授权。同时，根据节点加入联盟链的认证机制，系统根据节点的地理位置信息选取 $m$ 个不同地理位置的节点作为临时共识节点，并假设物联网-区块链应用上线前的节点均为离线状态，以节点对预备管理节点的响应速度为分组依据，将节点划分为 $m$ 个共识集。以下是节点分组初始化算法的具体描述。

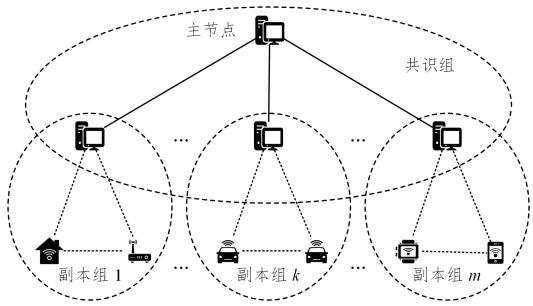


图 2 分组策略图

Fig. 2 Diagram of grouping strategy

1)临时共识节点 $c\in NC_1,NC_2,\cdots,NC_m$ 向其他节点发起副本组问询消息〈*RGROUP-ASK*，$n_c$，$g_h$，$rg$，$S_c$〉，$n_c$ 是临时共识节点编号，$g_h$ 是地理位置哈希值，$rg$ 是副本组编号，$S_c$ 是临时共识节点 $c$ 的签名。

2)节点 $i$ 收到副本组问询消息，首先验证消息签名的正确性，其次判断消息中的地理位置哈希值与节点自身的地理位置哈希值是否一致，如果一致则向临时共识节点回复副本组加入消息〈*RGROUP-ADD*，$n_i$，$g_h$，$S_i$〉，其中 $n_i$ 是节点编号，$g_h$ 是地理位置哈希值，$S_i$ 是节点 $i$ 的签名。

3)临时共识节点 $c$ 验证消息签名的正确性，若正确则将节点加入到副本组成员列表 *rgList* 中。副本组划分完毕后，将副本组成员列表 *rgList* 发送给副本组下的所有节点。

4)副本组分组结束时，临时共识节点的分组任务结束，并通过共识节点选取机制在副本组内重新选取共识节点，由于分组初始化缺少可以参考的信誉信息，共识节点在初始阶段也通过主节点选取机制选取主节点。注意，如果有节点需要加入区块链系统中参与共识，则只需要再次执行步骤 1)和步骤 2)即可。

4.2.2 节点选取机制

在 BDBFT 共识算法中，当共识组消息不能达成一致或视图的生命周期结束时，共识节点把其任期内收集的信誉信息广播给其所在副本组的所有节点，帮助副本节点更新其信誉预测模型。共识节点选取机制和主节点选取机制如下。

1)主节点选取机制

假设共识组内节点数量为 $G$，当前视图编号为 $V$，*CNID* 表示共识节点的编号，主节点的选取计算式如式(13)所示：

$$CNID=(V+1)\%G \tag{13}$$

2)共识节点选取机制

BDBFT 根据信誉预测模型和投票机制替换共识节点，预测概率越高则当选为共识节点的概率就越高。共识节点选取机制的具体步骤如下：

(1)节点通过本地部署的信誉预测模型，维护一个预测概率列表 *predList*。节点对在该列表中排名前三的节点进行投票，投票消息为〈*CGROUP-VOTE*，$n_v$，$S_i$〉，其中 $n_v$ 表示推荐委任主节点的节点编号，$S_i$ 则是节点签名。

(2)归票期间，如果收到来自不同共识节点的票数达到共识节点总数的一半以上，则认定投票有效。

(3)票数获得最多的主节点在共识组中发送数据同步请求〈*CGROUP-SYN*，$n_p$，$g_h$，$d$，$S_p$〉，其中 $n_p$ 是主节点编号，$g_h$ 表

示主节点的地理位置哈希值，$d$ 是需要同步的数据，$S_p$ 是主节点签名，共识节点收到同步消息，检查消息中是否存在错误，如果没有异议，则更新备份数据。

BDBFT 共识算法通过实现共识组和副本组共识，以达成物联网-区块链应用所有节点间的共识。对于 BDBFT 算法的一致性协议，新区块由共识组内的节点投票产生，再通过共识组成员节点发送给副本组的所有节点共识结果。BDBFT 算法的算法流程如图 3 所示，具体算法如算法 1 所示。BDBFT 算法 7 个阶段的一致性协议如下。

**算法 1**　BDBFT 消息一致性算法

输入：节点$N_i$，交易请求〈REQUEST〉

输出：共识结果〈REPLY〉

```
1. WHILE receive and verify〈REQUEST〉 THEN:
2.    IF isPrimary(N_i) THEN:
3.       startTime←time. Timestamp()
4.       broadcast〈PRE-PREPARE〉
5.    ElSE THEN:
6.       receive〈PRE-PREPARE〉
7.          startTime←time. Timestamp()
8.     IF 〈PRE-PREPARE〉=true THEN:
9.       broadcast〈PREPARE〉
10.   WHILE receive〈PREPARE〉 THEN:
11.      IF 〈PREPARE〉=true THEN:
12.         prepareCount++
13.      IF prepareCount>2f THEN:
14.         ts←getTransaction(〈REQUEST〉)
15.         execute(ts)
16.         endTime←time. Timestamp()
17.         g_h←Geohash(N_i)
18.         packup(〈COMMIT〉,g_h,endTime)
19.         broadcast〈COMMIT〉
20.   END WHILE
21.   WHILE receive〈COMMIT〉 THEN:
22.      IF 〈COMMIT〉=true THEN:
23.         commitCount++
24.         evaluateNode(〈COMMIT〉)
25.      IF commitCount>2f+1 THEN:
26.         broadcastToReplica〈REPLY〉
27.         replyToClient〈REPLY〉
28.   END WHILE
29.  END WHILE
```

1）REQUEST 阶段：客户端 $c$ 发起事务请求，并向主节点 $p$ 发送请求消息$\langle REQUEST,o,t,c\rangle\sigma_c$。

2）PRE-PREPARE 阶段：主节点接收到客户端发送的事务请求消息并进行合法性验证，若验证通过则给事务请求分配在视图 $v$ 中的唯一的序列号 $n$，对消息签名后向共识节点广播预准备消息$\langle\langle PRE\text{-}PREPARE,v,n,d\rangle\sigma_p,m\rangle$。

3）PREPARE 阶段：共识节点验证主节点发送的预准备消息，将消息写入本地日志并告知其他节点已收到此消息，请求验证该消息序列号与事务请求内容是否对应，对消息签名后向其他共识节点广播准备消息$\langle PREPARE,v,n,d,i\rangle\sigma_i$。

4）COMMIT 阶段：节点验证来自其他共识节点的准备消息，如果收到来自 $2f$ 个不同共识节点的准备消息，则将地理位置哈希值$g_h$和事务完成的时间戳 $t$ 打包到消息中，执行消息的事务请求并广播确认消息$\langle COMMIT,v,n,g_h,t,d,i\rangle\sigma_i$。

5）REPLY 阶段：若节点收到 $2f+1$ 个来自不同共识节点的确认消息，则认为事务请求的共识已经达成，将确认消息中的地理位置哈希值$g_h$和事务完成的时间戳 $t$ 输入到预测模型中，对节点共识行为进行评估；最后向客户端和副本组成员节点广播共识结果$\langle REPLY,v,t,c,i,g,r\rangle\sigma_i$。若客户端收到来自 $f+1$ 个共识节点的正确回复，则认为事务请求已经得到执行；同样地，若副本节点收到组内唯一共识节点的回复消息，则执行相应的事务请求。

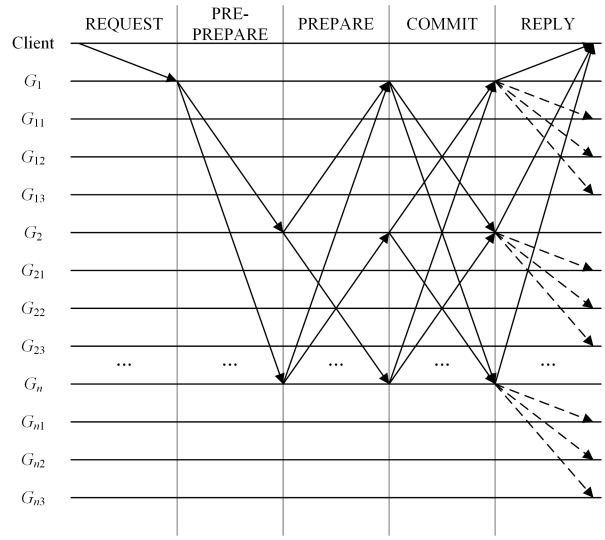


图 3　BDBFT 算法的流程

Fig. 3　Workflow of BDBFT algorithm

## 5　实验与结果分析

### 5.1　实验环境

实验基于 Go 编程语言模拟一个小型区块链系统，线程通过监听不同的端口代替节点，通过开启多个线程模拟共识节点的通信过程，系统中分别实现 PBFT 算法、LRBFT 算法[19]和 BDBFT 算法，分别从交易时延、吞吐量、通信开销和安全性 4 个方面评估 BDBFT 算法的性能，实验软硬件配置信息如表 2 所列。

表 2　实验配置信息

Table 2　Experimental configuration information

| 对象 | 配置 |
|---|---|
| 操作系统 | Windows 11 |
| 处理器 | Intel(R) Core(TM) i7-10750H 2.6 GHz |
| 内存 | 16 GB |
| 软件环境 | VsCode |
| Golang | v1.18.3 |

### 5.2　实验结果分析

#### 5.2.1　共识时延

共识算法的共识时延指客户端从发起事务请求到事务完成所经过的时间间隔。时延的大小直接影响系统的吞吐量和性能稳定性。假设 $Time_{\text{confirm}}$ 是事务完成时间，$Time_{\text{request}}$ 是发

起事务请求时间，则共识算法的时延计算式如下：

$$Delay = Time_{\text{confirm}} - Time_{\text{request}} \tag{14}$$

实验测试 PBFT 算法、LRBFT 算法和 BDBFT 算法在分组数为 40，60 和 80 时的共识时延指标。在保证其他条件不变的情况下，设置实验对照组的节点数量为 40，64，88，112，136 和 160，客户端以固定的时间间隔发送 20 次事务请求，每组实验重复 10 次，实验最终结果取 200 次事务请求时延的平均值。

如图 4 所示的实验结果表明，在节点数量相同的情况下，BDBFT 算法明显优于 PBFT 算法和 LRBFT 算法。可以看出，随着节点数量的增加，PBFT 算法达成共识的通信时延呈指数级增长，LRBFT 算法通过节点角色划分减少参与共识的节点数量，议员节点负责消息的共识，监督节点负责监督共识过程，与 PBFT 算法对比有效缩短了消息达成共识的时间，当节点数量规模变大时，由于监督节点的监督行为对共识过程的影响，共识时延也会随之增加。BDBFT 算法共识时延的增长速率明显低于 PBFT 算法和 LRBFT 算法，BDBFT 算法由于分组策略有效地减少了参与共识的节点数量，在节点数量增长到与分组数相等时，节点数量的增加对共识时延的影响较小；同时，对于 BDBFT 算法，分组数对于其共识时延的影响显著，当系统初始化过程中设置的分组数量增加时，参与共识的共识节点数量也会随之增加，进而也会造成 BDBFT 算法的共识时延增加，尽管如此，在系统节点数量不变的情况下，BDBFT 算法的共识时延仍远小于 PBFT 算法。因此，BDBFT 算法由于其分组策略和优化的一致性协议，在大规模网络节点中能够有效地降低共识的通信时延。

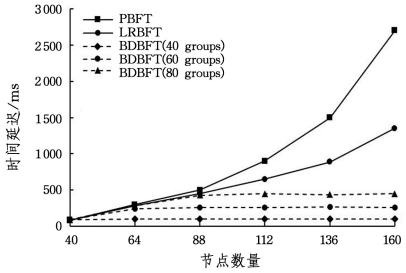


图 4 共识时延对比结果

Fig. 4 Comparison results of consensus delay

### 5.2.2 吞吐量

在区块链系统中，吞吐量(Transaction Per Second，TPS)是单位时间内完成的事务数量，是共识算法性能评估过程中的一个重要指标，高吞吐量系统往往意味着能够在给定时间内处理更多的事务。假设 $Transactions_{\Delta t}$ 表示共识算法在时间段 $\Delta t$ 中完成的事务总量，则吞吐量计算式如式(15)所示：

$$TPS = \frac{Transactions_{\Delta t}}{\Delta t} \tag{15}$$

实验测试 PBFT 算法、LRBFT 算法和 BDBFT 算法在分组数为 40，60 和 80 这 3 种分组情况下的吞吐量指标。设置系统总节点数量为 40，64，88，112，136 和 160，每批次事务总量为 100，重复实验 50 批次，结果取 50 批次实验的平均值，PBFT 算法、LRBFT 算法和 BDBFT 算法的吞吐量性能实验结果如图 5 所示。

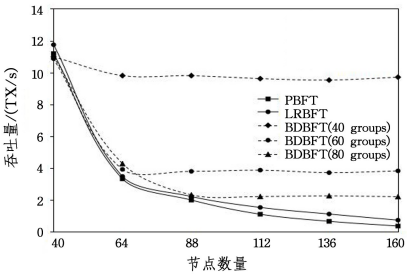


图 5 吞吐量对比结果

Fig. 5 Comparison results of throughput

由图 5 可知，随着节点数量的增加，各算法的事务处理能力均有所提升。PBFT 算法的吞吐量在节点数量递增的初期，其吞吐量下降幅度极大，但在节点数量增加到 64 以后，吞吐量下降的幅度逐渐平稳；LRBFT 算法通过改进拉格朗日插值法优化节点选举过程，通过选举议员节点和监督节点来减少参与共识过程的节点数量，其吞吐量性能虽优于 PBFT 算法，但监督行为会因为节点数量的增多而消耗更多的系统资源，影响了吞吐量性能。对于 PBFT 算法和 LRBFT 算法，在节点数增加的情况下，吞吐量仍然处于下降趋势。对于 BDBFT 算法来说，节点数在达到分组数(40，60，80)以前，节点数量的增加会严重影响吞吐量性能，但是在节点数达到分组数(40，60，80)以后，由于分组策略的影响，共识节点数量不再增加，增加的节点只能作为副本节点加入系统，因此不会影响共识过程，也不会影响吞吐量性能。因此，BDBFT 共识算法具有更好的扩展性和事务处理能力，可以在大规模网络节点中保持稳定的吞吐量性能。

### 5.2.3 通信开销

通信开销指在分布式系统中，为达成共识而进行节点间通信所产生的通信量。假设 PBFT 算法中的节点总数为 $N$。PRE-PREPARE 阶段，主节点向所有副本节点广播 PRE-PREPARE 消息，通信次数为 $N-1$。PREPARE 阶段，副本则需要向除自身之外的所有节点发送 PREPARE 消息，通信次数为 $(N-1)^2$。COMMIT 阶段，每个节点向其他节点广播 COMMIT 消息，通信次数为 $N\times(N-1)$。REPLY 阶段，节点向客户端发送共识结果，通信次数为 $N$。因此，汇总得到 PBFT 算法达成消息一致性所需的通信总数如式(16)所示：

$$N_{\text{PBFT}} = N-1+(N-1)^2+N\times(N-1)+N \tag{16}$$

假设 BDBFT 算法中的节点总数为 $N$，副本组的数量为 $G$，节点地理位置分布均匀，即所有副本组内的节点数量一致，则副本组内的节点数可以表示为 $\frac{N}{G}$ 且 $G+\frac{N}{G}<N$。PRE-PREPARE 阶段，共识组中的主节点将预准备消息发送给共识组成员，通信次数为 $G-1$。PREPARE 阶段，共识组成员节点广播预准备消息，通信次数为 $(G-1)^2$。COMMIT 阶段，共识组内的所有节点广播提交消息给除自己外的所有节点，通信次数为 $G\times(G-1)$。REPLY 阶段，共识节点发送共识结果给所有副本节点，通信次数为 $N-G$，同时向客户端发送共识结果，通信次数为 $G$，由此可得，在 REPLY 阶段的通信总次数是 $N$。因此，汇总得到 BDBFT 算法达成消息一致性所需的通信总数如式(17)所示：

$$N_{\mathrm{BDBFT}}=G-1+(G-1)^2+G\times(G-1)+N \tag{17}$$

图 6 给出了 PBFT 和分组数为 60 的 BDBFT 算法的通信开销。可以看出，PBFT 算法的通信开销随着节点数的递增而迅速提高，当区块链网络的规模扩大到大数量级的节点数量时，PBFT 算法会更快地增加通信成本。相比之下，BDBFT 算法在节点数为 60 时，通信开销达到上限值，即 1 000 kB。PBFT 算法的平均通信开销为 2 746.5 kB，BDBFT 算法的平均通信开销为 882.477 kB，BDBFT 算法相较于 PBFT 算法的通信开销降低了 67.87%。

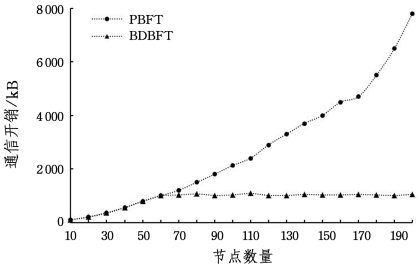


图 6　通信开销对比结果

Fig. 6　Comparison results of communication expense

### 5.2.4　安全性分析

传统的 PBFT 共识算法缺乏节点信誉评估机制，系统中存在的拜占庭节点始终能够选举主节点和参与共识过程，导致系统的安全性得不到保障。提出的 BDBFT 算法引入细粒度的基于 Dirichlet 分布的信誉预测模型，如果拜占庭节点在共识过程中作恶，其作恶行为会被评估为低信誉等级，在重新选举共识组时，拜占庭节点选举为共识节点的概率将会降低，从而减少共识组中拜占庭节点数量，提升系统的安全性。

假设所有节点的地理位置分布均匀，节点总数为 200，副本组的数量分别设置为 40，60 和 80，实验设置初始时共识组内拜占庭节点数量为 30，视图的生命周期为 20 轮共识，设置信誉值计算权重参数为 $\delta=0.5$，实验进行 60 轮共识，每轮共识后，统计共识组内拜占庭节点数量，实验结果如图 7 所示。

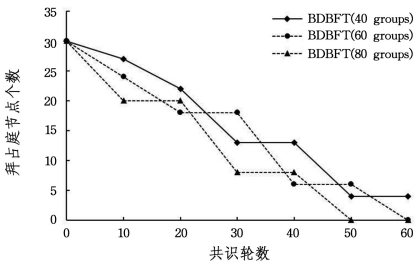


图 7　拜占庭节点数对比结果

Fig. 7　Comparison results of the number of Byzantine nodes

由图 7 的拜占庭节点数对比结果可以看出，当拜占庭节点数量 $f$ 与共识组内节点数量 $G$ 的数量关系不满足达成共识的条件 $G>3f+1$ 时，诚实节点根据获取的信誉信息对节点进行评估，重新选举共识组节点。当拜占庭节点数量占节点总数的比例越大时，诚实节点获取的信誉信息就会越少，拜占庭节点数量减少的幅度就会更低；当共识组内拜占庭节点降低到共识可以达成时，拜占庭节点的作恶行为将不会影响共识结果，共识组会伴随视图生命周期的结束而重新选举，在视图生命周期尚未完成时，拜占庭节点的数量不会减少，即如图 7 中曲线平缓部分所示。随着共识次数的增加，BDBFT 共识算法中共识组内的拜占庭节点数量呈下降趋势，直至拜占庭节点数为 0，因此 BDBFT 算法提升了系统的安全性。

### 5.2.5　共识算法对比分析

当前共识算法主要分为证明类（Proof of X，PoX）共识算法和拜占庭容错类（Byzantine Fault Tolerance，BFT）共识算法。表 3 列出了这两类主流共识算法与 BDBFT 共识算法分别在吞吐量、资源消耗量、可扩展性和去中心化程度方面的对比。

表 3　共识算法的对比

Table 3　Comparison of consensus algorithms

| 共识机制 | 吞吐量 | 资源消耗 | 可扩展性 | 去中心化程度 |
|---|---|---|---|---|
| PoW | 低 | 高 | 高 | 高 |
| PoS | 中 | 低 | 高 | 高 |
| DPoS | 中 | 低 | 高 | 高 |
| PBFT | 高 | 低 | 低 | 中 |
| DBFT | 高 | 低 | 中 | 中 |
| BDBFT | 高 | 低 | 高 | 中 |

表 3 表明，PoX 类共识算法的去中心化程度和可扩展性优于 BFT 类共识算法，这是因为 PoX 类共识算法要求节点遵守证明规则以竞争出块权，节点数量规模越大其去中心化程度越高，但证明规则的不同会带来资源浪费和吞吐量低的问题。BFT 类共识算法通过弱化去中心化程度来提升共识效率和降低资源消耗，但其通信复杂度高、可扩展性低。BDBFT 共识算法在 PBFT 共识算法的基础上，引入基于信誉预测模型和分组策略来减少参与共识的节点规模，有效解决了 PBFT 共识算法的可扩展性低的问题，同时提高了节点质量，避免拜占庭节点参与共识过程，保障了系统的安全性。

**结束语**　在物联网-区块链应用中，物联网节点具有性能低、能耗低和数量级高的特点，使用 PBFT 共识算法面临可扩展性低和通信开销高的挑战。本文提出了一种引入基于 Dirichlet 分布的细粒度信誉预测模型和分组策略的拜占庭容错（BDBFT）算法。BDBFT 算法首先通过引入基于 Dirichlet 分布的细粒度信誉预测模型来降低拜占庭节点参与共识过程的概率，保证主节点的可靠性，最大程度地保证系统的安全性；其次提出分组策略，将大规模网络节点划分为多个副本组和一个共识组，并允许节点动态加入物联网-区块链应用中，在降低通信复杂度的同时提高可扩展性和共识效率。实验结果表明，本文提出的 BDBFT 算法相较于 PBFT 算法，减少了通信开销和交易延迟，增加了系统吞吐量，提升了系统安全性。但是，BDBFT 算法仍存在一些问题，如分组数和信誉预测模型的平衡问题，共识节点数量多则会导致信誉预测模型计算消耗时间增加，导致系统开销有所增加。后续研究将继续改进 BDBFT 算法，以提供更安全、高效的物联网-区块链应用服务。

## 参 考 文 献

[1]　AL-SADAWI A，HASSAN M S，NDIAYE M. A survey on the integration of blockchain with IoT to enhance performance and eliminate challenges[J]. IEEE Access，2021，9：54478-54497.

[2]　RAJASEKARAN A S，AZEES M，AL-TURJMAN F. A com-

prehensive survey on blockchain technology[J]. Sustainable Energy Technologies and Assessments, 2022, 52: 102039.
[3] ABED S E, JAFFAL R, MOHD B J. A review on blockchain and IoT integration from energy, security and hardware perspectives [J]. Wireless Personal Communications, 2023, 129(3): 2079-2122.
[4] CHEN Y, LU Y, BULYSHEVA L, et al. Applications of blockchain in industry 4.0: A review[J]. Information Systems Frontiers, 2024, 26(5): 1715-17291.
[5] ZEKIYE A, ÖZKASAP Ö. The Internet of Energy Systems: Blockchain and Smart Contracts meet Federated Learning[C]// 2023 IEEE International Conference on Blockchain and Cryptocurrency(ICBC). IEEE, 2023: 1-3.
[6] SINGH D S, DWIVEDI R K. Blockchain Enabled Autonomous Vehicle Based Vehicular IoT System[C]// 2023 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics(IITCEE). IEEE, 2023: 762-767.
[7] ABDELLATIF A A, SAMARA L, MOHAMED A, et al. Medge-chain: Leveraging edge computing and blockchain for efficient medical data exchange[J]. IEEE Internet of Things Journal, 2021, 8(21): 15762-15775.
[8] TAN P L, WANG R S, ZENG W H, et al. Overview of Blockchain Consensus Algorithms[J]. Computer Science, 2023, 50(S1): 691-702.
[9] GERVAIS A, KARAME G O, WÜST K, et al. On the security and performance of proof of work blockchains[C]// Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. 2016: 3-16.
[10] SALEH F. Blockchain without waste: Proof-of-stake[J]. The Review of Financial Studies, 2021, 34(3): 1156-1190.
[11] LI C, XU R H, LI D. Characterizing Coin-Based Voting Governance in DPoS Blockchains[C]// Proceedings of the International AAAI Conference on Web and Social Media. 2023: 1148-1152.
[12] ZHANG G, PAN F, MAO Y, et al. Reaching consensus in the Byzantine empire: A comprehensive review of bft consensus algorithms[J]. ACM Computing Surveys, 2024, 56(5): 1-41.
[13] WANG Q, YU J S, PENG Z N, et al. Security Analysis on dBFT protocol of NEO[C]// International Conference on Financial Cryptography and Data Security. Cham: Springer, 2020: 20-31.
[14] 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.
[15] QUSHTOM H, MIŠIĆ J, MIŠIĆ V B, et al. A Two-Stage PBFT Architecture With Trust and Reward Incentive Mechanism[J]. IEEE Internet of Things Journal, 2023, 10(13): 11440-114524.
[16] XU J, ZHAO Y, CHEN H, et al. ABC-GSPBFT: PBFT with grouping score mechanism and optimized consensus process for flight operation data-sharing[J]. Information Sciences, 2023, 624: 110-127.
[17] WANG Z F, REN Y W, CAO Z Y, et al. LRBFT: Improvement of practical Byzantine fault tolerance consensus protocol for blockchains based on Lagrange interpolation[J]. Peer-to-Peer Networking and Applications, 2023, 16(2): 690-708.
[18] WANG Z F, LIU S Q, WANG P, et al. BW-PBFT: Practical Byzantine fault tolerance consensus algorithm based on credit bidirectionally waning[J]. Peer-to-Peer Networking and Applications, 2023, 16(6): 2915-2928.
[19] XU G Q, BAI H P, XING J, et al. SG-PBFT: A secure and highly efficient distributed blockchain PBFT consensus algorithm for intelligent Internet of vehicles[J]. Journal of Parallel and Distributed Computing, 2022, 164: 1-11.
[20] HUANG B H, PENG L, ZHAO W H, et al. Practical Byzantine Consensus Algorithm Based on Verifiable Random Functions [J]. Computer Science, 2023, 50(S1): 737-742.
[21] KUMAR A, VISHWAKARMA L, DAS D. R-PBFT: A secure and intelligent consensus algorithm for Internet of vehicles[J]. Vehicular Communications, 2023, 41: 100609.
[22] LIU S N, ZHANG R H, LIU C Z, et al. P-PBFT: An improved blockchain algorithm to support large-scale pharmaceutical traceability[J]. Computers in Biology and Medicine, 2023, 154: 106590.
[23] MA W G, WANG Y C, HU D F, et al. E-PBFT: An Improved Consensus Mechanism Based on PBFT[C]// 2023 International Conference on Networking and Network Applications(NaNA). IEEE, 2023: 143-149.
[24] CHEN Y X, JIA Y P. DT-PBFT: A Double-Layer Group Consensus Algorithm of Credibility for IoT Blockchain[C]// 2023 2nd International Conference on Big Data, Information and Computer Network(BDICN). IEEE, 2023: 292-299.

**WANG Pu**, born in 1998, postgraduate. His main research interests include blockchain technology and consensus algorithm.

**SONG Zheli**, born in 1983, postgraduate, associate professor. Her main research interests include big data and blockchain technology.

(责任编辑:喻藜)