面向联盟链的优化 PBFT 共识算法

曹碧娟[1] 黄迎春[1]
CAO Bijuan HUANG Yingchun

摘 要 针对联盟区块链中的 PBFT（practical byzantine fault tolerance）共识算法存在着时延高、吞吐量低的问题，提出了一种基于实用拜占庭容错算法思想的优化共识算法。引入信任评估机制，将节点的整体信任度分为原始信任度与共识信任度。根据节点整体信任度，选择一组信任值较高的节点作为共识集群，从中使用概率模型方法选择主节点，执行三阶段协议时，采用批处理消息的方法提高算法性能，并加入升降级机制，保证节点可动态地参与更新。仿真结果表明，与 SPBFT 相比，所提出的算法交易平均时延降低 56%，消息平均吞吐量提升 49%。

关键词 联盟链；共识算法；PBFT；信任评估机制；批处理

doi：10.3969/j.issn.1672-9528.2024.10.033

0 引言

共识层是联盟链的核心，共识算法可使高度分散的节点在去中心化的网络中高效地针对区块数据的有效性达成共识。主流的共识算法有：POW（proof of work）、POS（proof of stake）、PBFT（practical byzantine fault tolerance）共识机制。POW 工作量证明机制是只有通过大量计算和消耗大量资源的参与者才能获得权利，从而减少恶意行为的可能性，但网络性能太低、资源浪费、算力集中化 [1]。POS 股权证明机制是通过抵押一定数量的加密货币来获得记账权，必须通过购买的方式获得代币，提高了普通人获得加密货币的门槛，并且一旦权益最高的节点出现问题，就容易造成上链停滞 [2]。PBFT 拜占庭容错算法是指在分布式系统中允许一定数量的节点产生错误或者作恶，但仍能保证系统达成一致的特性 [3]。联盟链选择 PBFT 作为其共识机制，主要是因为它既满足一定的去中心化程度，又兼顾一定的性能。

目前联盟区块链 PBFT 共识算法存在交易时延高、吞吐量低的不足。叶博文等人 [4] 提出了一种基于二分 K 均值算法的改进 PBFT 共识算法。首先，获取节点地理坐标并计算节点综合评价值，通过二分 K 均值算法将节点划分为一个双层多中心聚类集群。然后，先在下层集群再在上层集群对区块进行 PBFT 共识。最后，集群验证执行并存储区块，完成共识，提升交易吞吐量，但此方法的交易时延还是很高。黄宇翔等人 [5] 在机器学习分类算法与 PBFT 共识算法的基础上，提出一种应用于供应链的区块链 PBFT 共识算法优化方法，对构建供应链与区块链的集成框架进行分析，根据供应链中参与共识的节点属性特征，运用 K- 近邻（K-nearest neighbors）来优化 PBFT 共识算法的主节点选取规则，降低交易时延，但此方法在吞吐量上无明显提升。针对上述问题，本算法在主节点选取上引入信任评估机制，运用线性规划与自适应粒子群优化算法（adaptive particle swarm optimization）确定原始信任度权重与共识信任度权重，得到整体信任度。根据整体信任度选出信誉值较高的节点组成共识集群，从中构建 Softmax 概率模型来表示每个节点成为主节点的概率，随机选取概率最大的作为主节点，执行三阶段协议时，在第二三阶段加入批处理打包消息的方法，并引入升降级机制，保证节点可动态地参与更新，降低算法交易时延，提升吞吐量。

1 改进共识算法

1.1 改进思路

在 PBFT 算法共识中需要选举一个主节点来领导共识过程，节点间的主节点选举会导致一定的延迟，若恶意节点担任主节点，不仅会浪费重新选取主节点的时间，还会降低系统的吞吐量。在共识的三阶段协议中节点之间会进行多轮消息交换以达成共识。每个阶段都涉及节点间的消息传递和验证，导致通信开销和节点的负担会显著增加，从而降低了系统的吞吐量。

若引入信任评估机制，节点会更加迅速和准确地进行验证，提高每个共识轮次验证效率，缩短整个共识过程的时间。当节点为了保持良好的信任度而减小不必要的通信时，整体网络负载就会降低，从而提升吞吐量。若 PBFT 执行三阶段

1. 沈阳理工大学信息科学与工程学院 辽宁沈阳 110159

协议时节点可并行处理多个请求，而不是依次处理每个单独请求，那么整体处理速度就会加快。

因此，本算法针对算法吞吐量低、时延高的问题，根据硬件环境指标为每一个节点分配一个原始信任度，表示节点的基础性能；在共识过程中，对节点的表现进行实时监控和评估，动态地调整节点的共识信任度；将节点的原始信任度和共识信任度分别赋予相应的权重，得出每个节点的整体信任度。根据整体信任度得出一组优组节点，信任度越高的节点被选为主节点的概率越大，但并非完全确定，防止出现长期垄断主节点职位的现象，从中建立 Softmax 概率模型随机选举主节点以完成共识过程，可有效降低恶意节点的影响，最后在三阶段协议中采用批处理方式处理消息，提高系统效率。

1.2 具体实现

（1）原始信任度（P）

原始信任度（P）为物理设备的基础性能，分别包括节点内存大小、节点 CPU 处理频率、节点硬盘容量。内存（P_1）：内存大小决定了节点能够处理的数据量和缓存大小，进而影响系统吞吐量；CPU 处理频率（P_2）：处理频率影响节点在执行共识算法、处理交易和区块验证的效率，进而影响系统时延、吞吐量；硬盘容量（P_3）：硬盘容量影响节点对区块链数据的存储能力。

分别设置权重为 λ_1、λ_2、λ_3，节点原始积分公式为：

$$P=\sum_{i=1}^{3}P_i\lambda_i \tag{1}$$

λ_i 的设定方法：原始信任度为系统物理状态，不应过大，否则会影响综合积分导致选取错误主节点，造成时延增加、吞吐量减少，所以确定权重 λ 值使原始信任度 P 最小化。

最小化：$P=\lambda_1\times P_1+\lambda_2\times P_2+\lambda_3\times P_3$

约束条件：

$$\lambda_1+\lambda_2+\lambda_3=1;\lambda_1,\lambda_2,\lambda_3>0;\lambda_2>\lambda_1>\lambda_3$$

当 λ_3=0.1、λ_1=0.2、λ_2=0.7、P=26.39 时，P 最小。节点原始信任度公式为：

$$P=0.2\times P_1+0.7\times P_2+0.1\times P_3 \tag{2}$$

（2）共识信任度（S）

共识信任度（S）是各个节点在共识时的情况表现。若节点被检测出为恶意节点，此节点的信任度为 0；若节点完成一次共识，则信任度加 1；若节点共识响应超时而不是作恶，则信任度加 0.5。

（3）整体信任度（Z）

整体信任度为原始信任度、共识信任度之和，设置原始信任度权重与共识信任度权重分别为 β_1、β_2。节点整体信任度为：

$$Z=\beta_1\times P+\beta_2\times S \tag{3}$$

β_1、β_2 设定方法：采用自适应粒子群优化算法（adaptive particle swarm optimization）。β_1、β_2 不是固定的数值，而是随着优化过程动态变化的 [6]。将节点的原始信任度作为目标函数的一部分，并将节点的共识信任度作为另一部分。利用 APSO 算法在权重空间中搜索，找到一组较优的原始信任度权重和共识信任度权重。通过实时监控和调整权重，系统可以更有效地选择主节点，减少时延，提高吞吐量。

通过进行 100 次交易次数仿真模拟得出，当 β_1=0.3、β_2=0.7 时，Z=77.917，此时系统性能最好，将此时综合积分设为迭代停止值。通过 APSO 算法寻找更为准确的 β_1、β_2。

（4）Softmax 函数

选择一组信任度较高的节点作为共识集群，Softmax 函数将每个输入的整体信任度（Z）转换为一个对应的概率 Z_i，计算方式为：

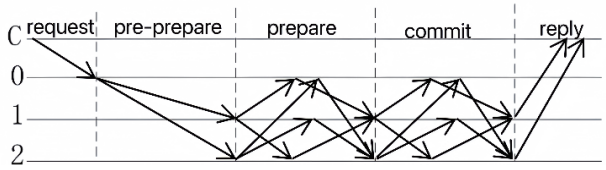
$$Z_i=\frac{e_i^{z_i}}{\sum_{j=1}^{n}e_j^{z_j}} \tag{4}$$

式中：Z_i 是输入的整体信任度第 i 个元素，e 是自然对数的底，n 是输入的节点个数 [7]。

Softmax 函数将输入的每个节点整体信任度（Z）转换为一个介于 0 和 1 之间的值，并且所有元素的和为 1。根据这个概率分布进行主节点随机选取。

（5）优化三阶段协议

主节点接收到来自客户端请求后，按照三阶段协议向全网广播消息。主要包括预准备（pre-pare）、准备（prepare）、提交（commit）三个阶段 [8]，其中 prepare、commit 阶段需要对每个节点传递的消息分别验证，十分浪费系统资源。采用批处理的方法发送打包好的消息给所有参与节点，节点在收到这个批处理消息后，不需要逐个处理请求，而是一次性处理整个批次请求。通过上述方法，可减少节点之间的通信次数，提高吞吐量。图 1 为采用批处理方法后的三阶段协议图。



（注：C 是客户端，0 是主节点）

图 1 优化后三阶段协议图

2 仿真结果分析

在本地主机上模拟区块链 PBFT 共识算法的交易过程，搭建一个仿真的消息交易网络，通过将消息进行 100 次请求

后，对改进后的 PBFT 进行仿真实验测试与分析。

2.1 交易时延仿真对比

交易时延是指客户端向主节点发送一个交易请求到客户端确认完成共识的时间间隔 [9]。实验中交易时延取 100 次交易的平均值，交易时延越低表示 PBFT 性能越好。图 2 为不存在拜占庭节点交易时间对比图。

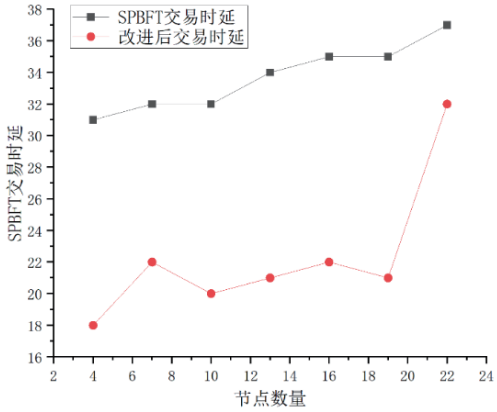


图 2 不存在拜占庭节点两种算法交易时延对比图

从图 2 中可以看出 SPBFT 和本算法改进的 PBFT 都是增长趋势，但本算法改进后的 PBFT 交易时延明显小于 SPBFT 的交易时延，且改进后的交易时延比 SPBFT 交易时延下降了 34%。

图 3 为存在拜占庭节点交易时间对比图，本算法改进的 PBFT 始终在 SPBFT 下方，改进后的交易时延比 SPBFT 下降了 78%。综上所述，改进后的 PBFT 的交易时延始终低于 SPBFT 的交易时延，平均交易时延降低 56%。

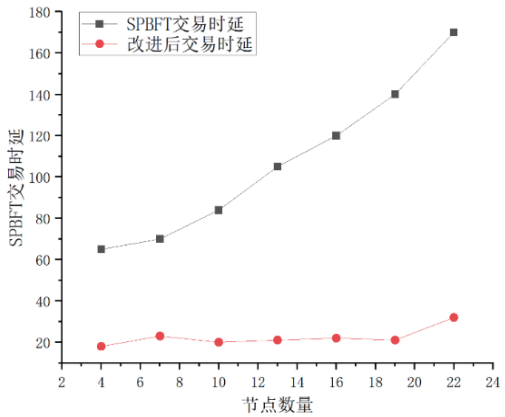


图 3 存在拜占庭节点两种算法交易时延对比图

2.2 消息吞吐量仿真对比

吞吐量指的是在单位时间内完成的交易的数量，一般用 TPS 来表示 [10]。消息吞吐量越高说明一段时间内 PBFT 处理的工作量越大。图 4 为两种算法在不同情况下的消息吞吐量对比图。

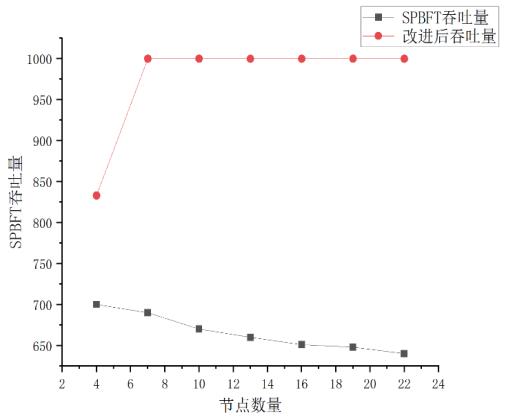


图 4 不存在拜占庭节点两种算法吞吐量对比图

图 4 为不存在拜占庭节点吞吐量对比图，改进后的 PBFT 共识算法吞吐量明显高于 SPBFT 共识算法吞吐量，因为 SPBFT 在主节点执行优化一致性协议后还需对共识节点的状态进行判断，但是在没有拜占庭节点的情况下，此动作是多余的。改进后的 PBFT 吞吐量比 SPBFT 吞吐量提升了 47%。

图 5 为存在拜占庭节点交易时间对比图，在同一时间内本文改进的 PBFT 吞吐量优于 SPBFT 吞吐量，并且在 7 个节点之后吞吐量一直保持稳定状态，改进后的吞吐量比 SPBFT 吞吐量提升了 51%。综上所述，改进后的 PBFT 吞吐量始终优于 SPBFT 吞吐量，吞吐量平均提升 49%。

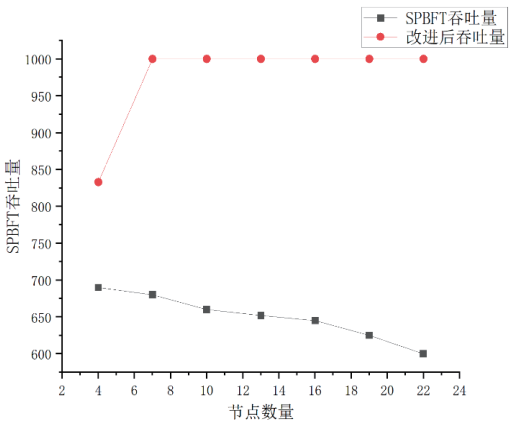


图 5 存在拜占庭节点两种算法吞吐量对比图

3 结论

基于 PBFT 算法的思想，提出一种优化的共识算法。引入原始信任度与共识信任度共同构成整体信任度，并加入概率模型和升降级机制，改变 PBFT 主节点的选取规则，在三阶段过程中采用批处理消息的方法，降低交易时延提高吞吐量。仿真结果表明，在相同的条件下，与 SPBFT 算法相比，优化后的 PBFT 算法平均交易时延比 SPBFT 降低 56%，消息平均吞吐量提升 49%。

参考文献：

[1] 隋星原，王峰．结合权益证明的工作量证明共识算法优化 [J]. 计算机仿真，2023,40(12):455-459+464.

[2] 商广勇，赵钦，陆冬妮，等．基于动态分组的主流区块链 PoS 共识算法研究 [J]. 现代电子技术，2023, 46(9):87-90.

[3] 高建彬，刘洋洋，夏虎，等．基于信誉分类的拜占庭容错共识算法 [J]. 无线电工程，2024,54(4):804-816.

[4] 叶博文，贾小林，顾娅军．面向物联网的改进 PBFT 共识算法 [J/OL]. 计算机系统应用，1-8[2024-03-13].https://doi.org/10.15888/j.cnki.csa.009455.

[5] 黄宇翔．应用于供应链的区块链 PBFT 共识算法优化 [J]. 计算机系统应用，2024, 33(4):209-214.

[6] 王震，张珊珊，邬斌扬，等．基于自适应粒子群优化算法的串联复合涡轮储能优化策略 [J]. 计算机应用，2024, 44(2): 611-618.

[7]KUMAR P D, BISWAJEET S, SUKADEV M. An efficient detection and classification of acute leukemia using transfer learning and orthogonal softmax layer-based model[J]. IEEE/ACM transactions on computational biology and bioinformatics, 2022, 20: 1817-1828.

[8] 王森，李志淮，贾志鹏．主节点随机选取的改进 PBFT 共识算法 [J]. 计算机应用与软件，2022,39(10):299-306.

[9] 刘泽坤，王峰，贾海蓉．结合动态信用机制的 PBFT 算法优化方案 [J]. 计算机工程，2023,49(2):191-198.

[10] 李帅，侯瑞春，陶冶．基于区块链的服务型制造供应链溯源技术研究 [J]. 制造业自动化，2023,45(4):196-203.

【作者简介】

曹碧娟（2000—），女，辽宁抚顺人，硕士研究生，研究方向：网络服务与信息安全。

黄迎春（1976—），男，辽宁瓦房店人，硕士，副教授，研究方向：网络服务与信息安全、嵌入式系统实时调度。

（收稿日期：2024-07-10）

（上接第 138 页）

在具有可控幂律的无标度拓扑演化模型中，通过引入节点度调节因子和适应度函数调节因子来保证网络的幂律分布在一定范围内可调，使得网络中的节点在失效时具有较好的容错性。在具有链路补偿机制的无标度拓扑演化模型中，首先通过对网络中能量小、距离大的节点和相应的链路进行选择性的删除，可以降低网络能耗；其次通过对失效链路进行适当补偿，增强了网络的自愈和重构能力，因此演化的网络拓扑具有很好的抗毁性。两个模型在网络构建和择优连接的过程中具有一致性，新加入簇头节点都是通过随机行走的方式确定其局域世界，并按照择优连接概率选择合适的簇头节点进行连接。两种模型构建的网络拓扑在能耗方面更加均衡，且网络的容错性和抗毁性得到了提升，延长了网络生命期。

参考文献：

[1]SHI W, HONG B. Task scheduling inbudget-constrained cloud computing systems to maximise throughput[J].International journal of computational science and engineering, 2012, 7(4):319-328.

[2]MATHIVILASINI S, SRIVATSA S K. A novel energy efficient for wireless hart applications[J]. Research journal of applied sciences engineering & technology, 2015,11(4):396-399.

[3] 陈力军，刘明，陈道蓄，等．基于随机行走的无线传感器网络簇间拓扑演化 [J]. 计算机学报，2009,32(1):69-76.

[4] 郑耿忠．无线传感器网络拓扑控制与优化研究 [D]. 西安：西安电子科技大学，2012.

[5] 符修文，李文锋．基于局域世界的无线传感器网络分簇演化模型 [J]. 通信学报，2015,36(9):204-214.

[6]CHEN C, XIN G, YU J, et al. IDUC: an improved distributed unequal clustering protocol for wireless sensor networks[J]. International journal of distributed sensor networks, 2015(5):682-693.

[7]BARABASI A L, ALBERT R. Emergence of scaling in random networks[J]. Science, 1999, 286(5439): 509-512.

[8] 刘洲洲，王福豹．能量有效的无线传感器网络无标度拓扑模型 [J]. 北京邮电大学学报，2015,38(1):87-91.

[9]LIN C H, TSAI M J. A comment on HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks[J]. IEEE transactions on mobile computing, 2006, 5(10):1471-1472.

[10]SARAMAKI J, KASKI K. Scale-free networks generated by random walkers[J]. Physica A, 2004 (341):80-86.

【作者简介】

王莹（1993—），女，河南开封人，硕士，助教，研究方向：计算机网络、大数据。

（收稿日期：2024-07-21）