基于组播通信的PBFT算法改进*

杨孝天，马　冉，李　江，高　飞
（西藏大学 信息科学技术学院，西藏 拉萨 850000）

摘　要： PBFT算法存在通信复杂度高、性能受节点增加而下降等问题，引入组播通信应用于RPBFT（基于角色的拜占庭共识机制），提出了一种通信复杂度低、可以动态分配共识节点、不因节点数增加而性能下降的WRPBFT共识算法。WRPBFT将节点划分为共识节点和候选节点两类节点，动态地选取参与共识的共识节点进行组播通信。实验与分析表明，WRPBFT共识算法可以动态地实现节点的划分与选取，并且相较传统PBFT算法，WRPBFT算法具备更高吞吐量、更低的时延和更低的通信复杂度。

关键词： PBFT；组播；P2P；区块链
中图分类号： TP315.69　　**文献标志码：** A　　**DOI:** 10.16157/j.issn.0258-7998.223075

中文引用格式： 杨孝天，马冉，李江，等. 基于组播通信的PBFT算法改进[J]. 电子技术应用，2023，49(2)：67-71.
英文引用格式： Yang Xiaotian，Ma Ran，Li Jiang，et al. Improvement of PBFT algorithm based on multicast communication[J]. Application of Electronic Technique，2023，49(2)：67-71.

Improvement of PBFT algorithm based on multicast communication

Yang Xiaotian，Ma Ran，Li Jiang，Gao Fei
(School of Information Science and Technology，Tibet University，Lhasa 850000，China)

Abstract： PBFT algorithm has some problems such as high communication complexity and performance decrease with the increase of nodes.This paper introduces multicast communication applied to RPBFT(role-based Byzantine consensus mechanism), this paper proposes a WRPBFT consensus algorithm with low communication complexity, which can allocate consensus nodes dynamically and does not degrade with the increase of the number of nodes.WRPBF divides nodes into consensus nodes and candidate nodes, and dynamically selects consensus nodes participating in consensus for multicast communication. Experiments and analysis show that WRPBFT consensus algorithm can dynamically achieve node partitioning and selection, and WRPBFT algorithm has higher throughput, lower delay and lower communication complexity compared with traditional PBFT algorithm.

Key words： PBFT；multicast；P2P；blockchain

0 引 言

区块链采用P2P（peer-to-peer）通信模式，P2P是一种分布式网络，节点之间可以直接进行信息交换。P2P为区块链提供高效、安全、通用的网络通信基础，支持区块链进行单播、组播和广播通信[1]。P2P具有如下功能：(1)标识区块链节点，每一个区块链节点都被唯一标识，区块链节点通过唯一的节点标识进行寻址；(2)管理网络连接，负责维护区块链节点之间的正常连接和异常连接；(3)消息发送，支持区块链消息进行单播、组播和广播；(4)同步状态，完成区块链节点间信息的同步。

PBFT算法起源于拜占庭将军问题，为解决拜占庭将军问题，Leslie Lamport提出了BFT（拜占庭容错算法）。基于BFT拜占庭容错算法，Miguel Castro(卡斯特罗)和Barbara Liskov(利斯科夫)于1999年提出了PBFT算法，将BFT算法复杂度从指数级降到多项式级，使得PBFT共识算法可应用于实际系统中[2]。PBFT作为一种共识机制被应用于区块链，相较主流共识机制POW[3] 10 min出一块，PBFT算法可以做到秒级确认交易，节约算力资源，并且可以容错1/3的错误节点（故障节点、欺骗节点等）。但是PBFT仍存在网络复杂度高、延迟高、性能随节点的增多而下降等问题。

当前学者就PBFT算法存在的问题做出了大量的研究，研究可以分为如下几类：通过分组来提高算法效率，如王谨东[4]提出使用K-medoids聚类算法将所有节点划分为多个节点簇，提出了一种基于PBFT与Raft改进的

* 基金项目：西藏自治区教育科学研究重点课题（xzjykt221008）

拜占庭容错共识算法K-RPBFT；引入信誉机制改善PBFT算法，如杨昕宇[5]提出一种基于演化博弈的理性实用拜占庭容错共识算法，基于信誉对共识节点进行划分；基于角色的PBFT算法改进，如李腾[6]提出一种基于角色管理的拜占庭容错（RPBFT）共识算法，首先将系统中的节点划分为管理者、候选者和普通节点3类具有不同职责的角色节点，通过分配不同节点不同的任务进而提高PBFT算法的效率。当前相关PBFT算法的研究大多数都是基于算法的优化[7-9]，进而提高算法的效率。本文从通信技术方面改进PBFT算法，引入组播通信应用于基于角色的PBFT算法[10-11]，优化PBFT共识算法，通过角色分配和组播通信两大技术实现动态地选取参与共识的节点，以解决传统PBFT共识算法存在高时延、高复杂性、不能处理大规模节点等问题。

1 算法设计

1.1 一致性算法

将原来相关节点广播的算法改为组内组播算法过程如图1所示，其中，×表示拜占庭节点，O表示非订阅节点，非订阅节点不参与共识。WRPBFT算法模块包括Request、Pre-request、Prepare、Commit、Reply 5个阶段，非订阅节点不参与共识过程。

(1) Request：客户节点发送Request请求。

(2) Pre-prepare：主节点收到客户节点发送的Request请求，产生签名包，并将签名包与Pre-prepare进行组播，发送给订阅节点。

(3) Prepare：收集签名包，节点收集满$2\cdot f+1$签名包后，开始广播Commit。

(4) Commit：收集Commit，节点收集满$2\cdot f+1$ Commit包，开始广播Reply。

(5) 统计Reply信息，统计完后将最新的区块提交至主节点。

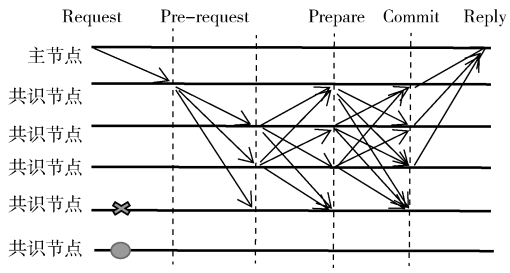

图1 一致性算法原理图

1.2 节点类型与共识节点选择

1.2.1 节点类型

节点包括以下4种：Client客户节点、Primary主节点、Replica共识节点、Candidate候选节点，其功能如表1所示。客户节点负责发送交易请求。主节点负责接收客户节点的交易请求，并进行交易打包，筛选参与本次共识的共识节点并发布订阅信息。每轮只有一个主节点，主节点也是共识节点，是由共识节点选举而出的。共识节点负责完成区块共识，共识节点有多个，每个共识节点都具有相同的处理过程。候选节点负责校验每个区块共识节点签名是否到达2/3，校验区块的执行结果是否一致。

表1 不同节点类型功能表

节点类型	功能
Client客户节点	发送交易请求
Primary主节点	由共识节点选出，负责接收客户请求、发布订阅信息、交易打包出块
Replica共识节点	负责区块共识
Candidate候选节点	校验区块执行结果

1.2.2 共识节点选择

参与共识算法的节点有共识节点和候选节点，共识节点负责执行PBFT共识算法，并具备成为主节点的资格。候选节点不具备成为主节点的资格，负责对共识节点的合法性验证，候选节点具备成为新的共识节点资格。共识节点也并不是一直保持不变，每经过i次共识，共识节点便与候选节点完成一次替换；并且可以动态地设置共识节点个数，达到动态配置共识节点。如图2所示，替换周期i通过设置替换周期。

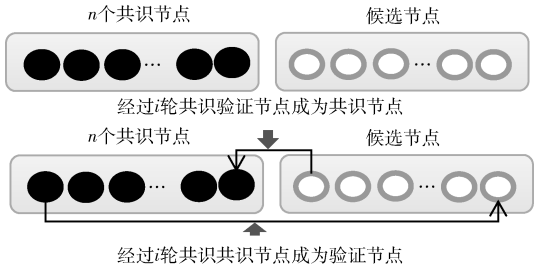

图2 共识节点选择核心思想图

1.3 组播通信通信模型

1.3.1 引入Topic

基于AMOP（Advanced Messages Onchain Protocol）链上信使协议，通过订阅Topic来实现节点间组播通信，引入组播通信包括以下两个部分：(1)共识节点执行PBFT共识算法的过程，从共识节点选取参与本次共识的r_c个共识节点进行节点间组播，组播完成PBFT共识算法Request、Pre-request、Prepare共识过程；(2)候选节点执行节点验证，采用组播通信的方式选择参与验证的节点。基于AMOP实现组播通信，AMOP支持点对点的实时通信，为区块链提供安全高效的消息传输信道，AMOP基于SSL通信加密，确保消息无法被窃听，消息收发均有异常重传、超时检测和路径规划机制，其实现

组播通信原理如图3所示：一个发送者，多个接收者。消息发送者（Message Queue消息队列是应用程序之间的通信方法）获取到连接以及Message Queue通道，绑定队列到交换机。每一个接收者都有自己的队列并绑定到交换机，消息发送者将信息发送到交换机。消息发送者发送的信息经过交换机到达队列，实现一个信息多个接收者获取的目的。

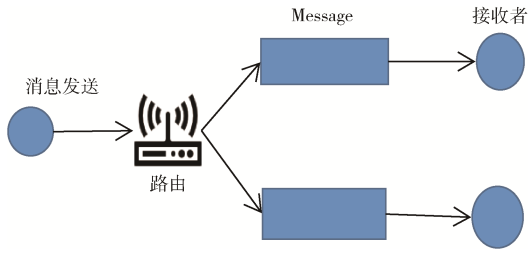

图3　组播通信原理图

1.3.2 引入索引列表

(1)通过索引列表添加订阅节点ID和Topic订阅信息，提高通信效率与管理效率；(2)考虑到节点ID与Topic（PBFT共识算法以公钥作为节点ID，一般是64 B）在共识过程中会消耗部分宽带，引入节点索引，可以减少通信过程中的带宽消耗。所有共识节点共同维护一份公共的共识节点与Topic列表，所有的候选节点共同维护一张公共的验证节点与Topic列表。节点列表记录了每个共识节点ID在这个列表中的位置，如图4所示，索引列表对节点进行重新的排序并添加排序编号，记录节点Topic订阅信息。发送消息时，只需要带上节点编号，其他节点即可以从公共的节点列表中索引出节点的ID和相应的组播信息实现区块链网络组播通信。

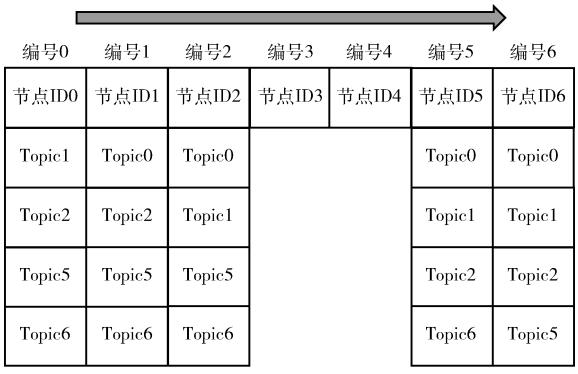

图4　索引列表原理图

2 算法实现

2.1 共识机制

(1) 选取共识节点：开始WRPBFT选取n个共识节点参与共识（共识节点列表为listR[n-1]），为确保去中心化和系统的安全性，每经过i轮的共识需要进行共识节点和候选节点的替换，确保每个节点都具备参与共识的权力。候选节点替换共识节点替换策略如下：将节点索引为list[i]的共识节点从共识节点中剔除，并加入(list[i].id$x$+K)%(n-1)对应候选节点作为新的共识节点。其中i为第i轮，list[i].id$x$为编号为i对应的节点索引，n为共识节点总数，K为出块数，%为取余操作。替换成功后从索引列表删除对应共识节点和加入新的共识节点。

$$R=(\text{list}[i].\text{id}x+K)\%(n-1) \tag{1}$$

(2) 选取主节点：PBFT共识过程中，共识节点轮流成为主节点，主节点选取策略如下：

$$P=(m+n+v)\%m \tag{2}$$

其中，m表示共识节点个数，n表示验证节点个数，v表示视图数。

(3) 选取进行组播通信节点：主节点选取后，主节点首先判断当前主节点与自己索引是否相同，相同则选取r_c个共识节点编号进行节点间相互订阅，订阅完成后进行节点之间的组播，根据共识节点索引列表listR[n-1]选取r_c个共识节点，选取策略如下：

$$W=(n+R_c)\%n \tag{3}$$

其中，n表示共识节点总个数，R_c表示在[0，n-1]内随机选取的数。

(4) 节点开始打包：首先获取最新的区块高度，并基于最高高度的区块产生新的区块，取最高区块作为当前区块的父哈希，记录当前时间为时间戳，交易记为空。从交易池中获取交易，添加为新的交易记录，组装成新的块，将新块添加到Prepare包中，向所有订阅节点进行组播，订阅节点收到后进行Pre-request阶段。

(5) Pre-request负责判断是否存在重复的Prepare包，判断当前节点处于的区块高度，当前节点区块的父哈希节点块是否正确，完成对区块的执行并组播签名包。

(6) 共识节点收到签名包后进入Prepare阶段对签名进行合法性判断并缓存合法的签名包，判断缓存的签名包是否达到2·f+1，若收集满则进行广播Commit包。

(7) 进入Commit阶段：Commit阶段负责判断Commit信息包是否合法，合法则缓存，若Commit信息包大于2·f+1，则向主节点发送Reply信息，产生新区快。

2.2 错误应对机制

(1) 主节点错误

如果主节点宕机、不发消息，或者发送错误编码、进行篡改信息等，触发view-change进行主节点重新选举，所有共识节点都参加投票，当有2f+1个共识节点投票，触发重选。选举策略如下：

$$p=(v+1+r_c)\%n \tag{4}$$

(2) 共识节点错误

由于采用的组播通信机制，本文已采用随机选取共

识节点来完成PBFT共识，导致拜占庭容错数量减少，即出现拜占庭容错问题会增多。为减少这类事情的发生，本文采取多次组播策略，如果出现这样的问题就进行再次组播(i表示选取参与验证的验证节点编号)。设置进行j轮组播后将不再进行组播，直接进行广播所有共识节点进行共识算法处理，应对策略如下：选取上一次参加共识的共识节点索引对应的下一个节点。

$$r = \text{listR}[i+1].idx \tag{5}$$

3 实验仿真

3.1 实验结果

实验是基于Python语言实现的PBFT算法，模拟多个节点之间进行PBFT共识算法，通过一台电脑模拟多个节点进行共识。实验可以人为地设定参与共识的共识节点规模，本实验设定WRPBFT共识节点的节点规模为节点规模1/10，参与组播节点规模为共识节点的1/3。

吞吐量能够反映出共识机制对事务并发的处理能力。在区块链系统中，吞吐量通常用区块链系统在单位时间内处理的交易总量(Transaction Per Second, TPS)表示，单位为t/s。实验对比处理不同个事务请求在PBFT算法与RPBFT和WRPBFT算法的吞吐量，如图5所示。由图可知，WRPBFT算法相较其他两种算法具备更高的吞吐量。这是因为更少的共识节点参与共识，共识过程处理的交易量较少，进而提高了算法的吞吐量。

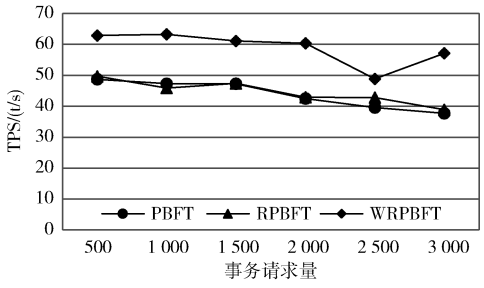

图5　算法吞吐量对比图

时延表示交易从客户端提交到交易被写入区块的时间差。如图6所示，对比PBFT、RPBFT、WRPBFT算法在不同事务请求规模情况下时延随处理请求事务的折线图。由图可得，随着处理事务量的增加，WRPBFT算法相较其他两种算法的时延更低，这是因为相同节点规模下WRPBFT算法更少的节点参与共识，节省了共识处理过程的时延。

共识过程信息量记录了request、pre_prepare、prepare、commit、reply、view_change发送的信息包之和，信息量反映网络通信复杂度情况。如图7所示，对比不同算法在共识过程处理信息量，WRPBFT算法在共识处理过程处理的信息量要低于传统的PBFT算法，有效降低了网络通信复杂度。

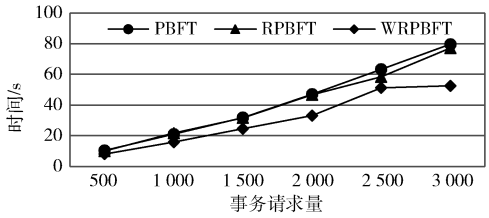

图6　算法时延对比图

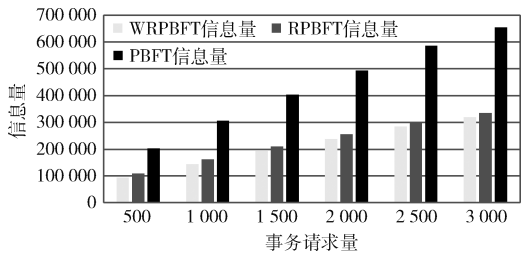

图7　算法信息量对比图

3.2 实验分析

(1) 时间复杂度不受节点规模的影响：客户节点进行组播复杂度为n_r，共识节点进行组播复杂度为n_r^2，共识Pre-prepare阶段杂度为n_r，共识Prepare阶段杂度为n_r^2，共识Commit阶段杂度为n_r^2，回复给客户节点杂度为n_r，所以总的时间复杂度为：$n_r+n_r^2+n_r+n_r^2+n_r^2+n_r=3\cdot n_r^2+3n_r=3n_r(n_r+1)$。共识算法复杂度是基于选取参与共识节点的规模，与总的节点规模无关，只与参与共识的共识节点规模有关。

(2) 带宽占用低：如果每个节点都进行信息的广播与转发可能会导致带宽被占满，导致系统瘫痪。本文采用组播通信模式：只取部分共识节点之间进行组播，以达成共识，可以有效节省带宽。在具有n个共识节点和m个候选节点的区块链系统中，采用组播进行选取$r_v<n$个共识节点，$r_c<m$个候选节点进行验证，假设共识一次信息大小为BS，在理想状态下每共识进行一次共识都需要向r_v个共识节点发送信息，共识节点带宽为$(r_v\cdot BS)$，$(r_v\cdot BS)<((n+m)\cdot BS)$。带宽不受节点规模影响而是随着$r_v$节点个数的减小而减小，WRPBFT可以将带宽降低为原来的$r_v/(n+m)$。虽然WRPBFT算法采用二进制标识对应索引表中Topic会增加通信信息量，可能会产生相应的时延。相应算法如下：假设共识规模为10 000个，则会增加100 00 bit的带宽。一个节点ID为64 B=64·1024 bit(1B=1024 bit，一个bit是计算机中的最小单位，简单的说就是一个0或一个1)相当于增加0.152个节点ID，仅仅增加在索引列表，几乎不影响算法性能。

(3) WRPBFT算法也存在以下缺点：如果选择参与共识的节点代表性低，将不能作为平均分布代表。因为参与共识的节点数量少，将会降低算法的容错率，并且出现共识错误后，处理共识错误复杂增加。其中容错性

分析如下：假设共有 N 个共识节点，拜占庭容错节点为 $1/n$，参与共识过程的共识节点选取规则为 $1/r$，则令参与共识节点个数为 $A=N\cdot(1/r)$，令拜占庭节点为 $B=N\cdot(1/n)$。出现拜占庭错误节点的概率为：

① 如果 $\lceil A\cdot(1/3)\rceil > B$，则出现概率为 0，可以安全地进行共识；

② 反之 $\lceil A\cdot(1/3)\rceil \leqslant B$，则出现概率为：

$$p=\sum_{i}(B/A)^{i} \tag{6}$$

其中，$A\cdot(1/3)<i\leqslant B$。

4 结论

针对 PBFT 算法通信复杂度高、性能受节点增加而下降等问题，本文提出了一种改进的 WRPBFT 算法。通过实验仿真表明，WRPBFT 算法相较 PBFT 与 RPBFT 算法具有更高的吞吐量和更低的时延，且需要处理的信息量更少，性能不受节点数规模增加而下降。同时，本文也指出了 WRPBFT 算法存在容错率高的缺点，今后将在算法容错性方面展开研究。此外，本文在实验仿真过程中缺少实验仿真的细化，并不能做到所有理论都应用于实践，仿真实验有待进一步完善，希望各位学者能给出意见，共同探讨。

参考文献

[1] 吕婧淑,操晓春.基于比特币系统的隐蔽通信技术[J].信息安全学报,2021,6(2):143-152.

[2] 冯了了,丁滟,刘坤林,等.区块链 BFT 共识算法研究进展[J].计算机科学,2022,49(4):329-339.

[3] 邓小鸿,王智强,李娟,等.主流区块链共识算法对比研究[J].计算机应用研究,2022,39(1):1-8.

[4] 王谨东,李强.基于 Raft 算法改进的实用拜占庭容错共识算法[J/OL].计算机应用:1-10[2022-05-26].http://kns.cnki.net/kcms/detail/51.1307.TP.20220517.1131.009.html.

[5] 杨昕宇,彭长根,杨辉,等.基于演化博弈的理性拜占庭容错共识算法[J].计算机科学,2022,49(3):360-370.

[6] 李腾,程哲,贾东立,等.基于角色管理的实用拜占庭容错共识算法[J].计算机工程与科学,2022,44(2):237-243.

[7] Shen Xuemin, Liu Dongxiao, Huang Cheng,et al. Blockchain for transparent data management toward 6G[J].Engineering,2022,8(1):74-85.

[8] 陈立全,胡杰,顾朋鹏.基于阶段投票和门限签名的改进 PBFT 协议(英文)[J].Journal of Southeast University (English Edition),2022,38(3):213-218.

[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/OL].计算机工程:1-12[2022-10-24].DOI:10.19678/j.issn.1000-3428.0063464.

[10] 李腾.PBFT 共识算法的改进及其应用研究[D].邯郸:河北工程大学,2021.

[11] 余苏喆.基于智能合约的数字版权系统研究与应用[D].成都:电子科技大学,2020.

(收稿日期:2022-06-08)

作者简介：

杨孝天(1996-),男,硕士研究生,主要研究方向:区块链、网络安全。

马冉(1994-),女,硕士研究生,主要研究方向:数据挖掘、推荐系统。

高飞(1980-),通信作者,男,硕士,教授,主要研究方向:区块链、大数据处理、图像处理、网络安全,E-mail:337679107@qq.com。

扫码下载电子文档

版权声明