基于分组的实用拜占庭容错共识算法

吉桐萱 [1]
JI Tongxuan

摘 要 通过实验发现，实用拜占庭容错共识算法 PBFT（practical byzantine fault tolerance）在区块链共识算法中会导致大量的信息广播，从而浪费通信资源并降低效率。为了解决这些问题，引入了一种在没有拜占庭节点的情况下，通过对节点进行分组共识，对原始 PBFT 进行优化的新方案。这种改进后的方法主要由分组和达成共识两个步骤构成。首先，将全部节点进行归类划分各组，实现分组共识；然后，在每个组内达成共识；最后，每个组的负责人进行总体共识，大大提高了达成共识的效率。与 PBFT 算法相比，提出的共识算法可以将达成共识的时间复杂度从 $O(N^2)$ 降低到 $O((N/2)^2)$，有效地减少了网络的通信消耗，平均延迟从 18 s 降低到了 9 s，平均吞吐量由 758 tps 提升到了 1040 tps。

关键词 区块链；共识算法；实用拜占庭容错；PBFT 算法；分组共识

doi：10.3969/j.issn.1672-9528.2024.07.018

0 引言

区块链由特定的成员机制和一致性协议组成，是一种分布式数据库技术，且使用加密原语，具有数据共享、不可变和安全的特点。区块链和传统式的中心化的技术有所区别，它是一种去中心化的数据技术，可分布式地存储，以链条的形式将区块数据交易按顺序联系在一起，没有集中控制交易的中心机构。区块链上的每个节点都保留链上所有保留的副本，都可以成为每一笔交易的见证者 [1]。这样的存储方式，不仅保证了交易的可信性，还能有效防止中心机构的篡改，也使整个区块链网络更加健壮，不会因为中心机构的单点故障而造成整个系统的瘫痪，为解决传统行业内的痛点问题提供了方案。区块链中采用密码学的方法对信息进行加密存储，对于交易双方的身份信息，只有拥有特定权限的节点才能够查看 [2]。为了保证每一条记录都有追溯性以及真实有效，区块中的交易都是按照一定顺序进行存储，且相邻两个区块中靠后的那个区块必须包含前面那个区块的 Merkle 树的哈希值，这样区块链中的信息就不易被更改 [3]。

区块链是一个共享数据库，由于它的公开透明的特征，同样使“可以追溯”的特征在食品供应链上也有所应用。保险业同样应用了区块链技术，它的不可伪造和全程留痕的特点，为区块链技术奠定了信任基础。共识算法是区块链中的重要组成部分 [4]。共识机制是在互相不信任的环境下，只要信任区块链协议下的软件系统就可以实现交易。拜占庭容错协议（PBFT）是一种在联盟链内被普遍采用的共识机制，有效改善了拜占庭容错算法的低效问题。但是，PBFT 仍然面临一些明显的弱点，限制了其发展的空间。PBFT 的三阶段通信规程的最后两个阶段要求每个节点向系统内的其他所有节点发送信息，这增加了通信的难度 [5]。PBFT 对于被揭露为恶意的主节点，没有特定的处罚措施，只是依赖视图切换规程确保共识过程的进行，不法节点还是存在于系统之中，这同样对系统的安全度构成威胁。

1 共识算法研究现状

区块链是一个信息技术领域的术语。区块链共识算法是指在一个分布式且去中心化的区块链网络中，不同的节点对某个数据或交易状态达成共同认可的一种算法或协议。从去中心化角度，区块链可分为公有链、私有链和联盟链。联盟链主要以使用拜占庭容错机制的绝对一致性共识机制为代表。公有链主要是以工作量证明（PoW）、权益证明（PoS）、委托权益证明（DPoS）为代表 [6]。在国外，公有链的共识算法被大多数学者进行深入研究，为的就是提升它的性能，降低由消耗电力大所引起的资源浪费。在我国，目前区块链技术已被应用在很多领域，例如物联网、食物溯源、保险业、数字版权管理、能源交易以及智能合约等。国内的各大企业也都在自主研发各个应用场景的区块链平台。

2 相关理论

2.1 工作量证明算法

工作量证明算法（PoW）适用于公有链，主要涵盖解答和检验两个步骤。解答步骤需通过大规模复杂数学计算来

1. 大连交通大学软件学院 辽宁大连 116028

寻找一个答案，而检验步骤则是用基本的数学计算去核实答案的正确性，这一看似简单的过程却能在短时间内完成[7]。PoW 算法实现难度较小，因为节点通过穷举计算获得随机数值。PoW 算法被广泛使用，确保数据的一致性和准确性，这需要大量的计算能力和功耗。同时，出于对数据安全的考虑，PoW 算法的块生成时间较长，这也导致了 PoW 共识的效率降低[8]。算法流程如图 1 所示。

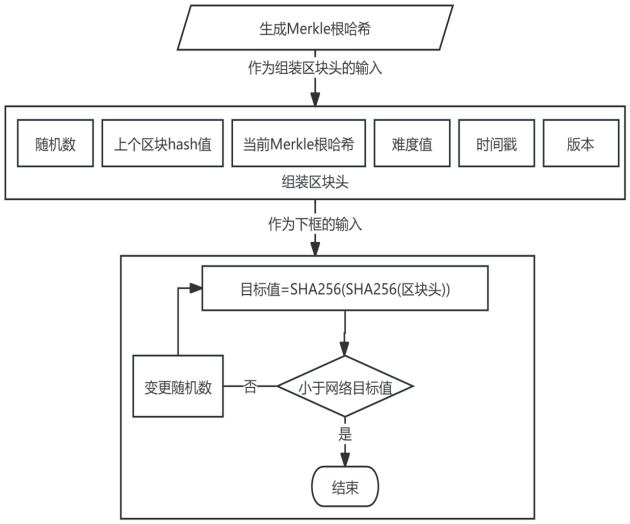

图 1 POW 算法流程图

2.2 股份授权证明算法

DPoS 共识协议的作用机制类似于一个公司的董事会决策模式，网络里的数字货币所有者就像股东，可以通过投票选举共识代表。其票数最多且愿意担当代表职务的前 101 个节点会被选入董事会[9]。这些董事会成员会按照预定的记账时间依次产出区块，如有代表在规定时间内未产生区块，他会被从董事会里解职。董事会的成员会在保养期（通常为 1 天）结束后进行一次更新。DPoS 算法结合了 PoS 算法和 PoW 算法的优点，不依赖于计算资源，从而降低了能耗。DPoS 共识协议相比 PoW 共识协议更有效率。不过，这种方法需要依赖数字货币才能达成共识，使得许多区块链应用难以采用 DPoS 算法[10]。

2.3 实用拜占庭算法（PBFT）

PBFT 算法的目的是确保在存在恶意节点的情况下仍然能够保证正确结果和一致状态。PBFT 算法不仅确保了系统的安全性和稳定性，还允许系统中存在的拜占庭节点不超过总数的三分之一[11]。拜占庭容错算法的复杂度是指数级别，由于 PBFT 的研究把复杂度降低到了多项式级别，这对于拜占庭容错算法是首次实现。在 PBFT 中的主节点（Primary）和备份节点（Backup）是参与共识过程的两类节点。客户端发送请求给主节点，并进行排序，同时所有的备份节点将会收到由主节点广播的消息，分界点再验收所接收到的消息的真实性，最终客户端收到这一系列操作得到的结果[12]。PBFT 算法中的核心部分是三阶段通信协议，它为共识结果的唯一性提供了保障。该三段协议又称为一致性协议，它是基于投票的共识协议，具体包括预准备（Pre-prepare）、准备（Prepare）、确认（commit）三阶段。

三种算法优缺点对比如表 1 所示。

表 1 PoW、DPoS 及 PBFT 优缺点对比

共识算法	执行时间 /s	TPS/s	拜占庭容错	可扩展性	代表应用
PoW	>100	<100	<1/2	强	Bitcoin
DPoS	<100	<1000	<1/2	强	EOS
PBFT	<10	<2000	<1/3	弱	Hyperledger

3 模型设计

对 PBFT 算法引入了一种分组机制，根据节点的数量将其分为四组。依照共识节点的状态决定运行哪种一致性协议，主要存在两个状态。

（1）在副主节点中并没有拜占庭节点，所有的拜占庭节点都存在于普通的节点中，因此，共识节点在该情况下会执行一致性优化协议。

（2）在副主节点里存在着拜占庭节点，此时 PBFT 算法的一致性协议都会被网络中所有的节点执行，以确保算法的容错能力。

3.1 优化一致性协议设计

如果网络中没有拜占庭节点，把节点间交互次数减少则优化共识效率，改进后算法的流程图如图 2 所示。

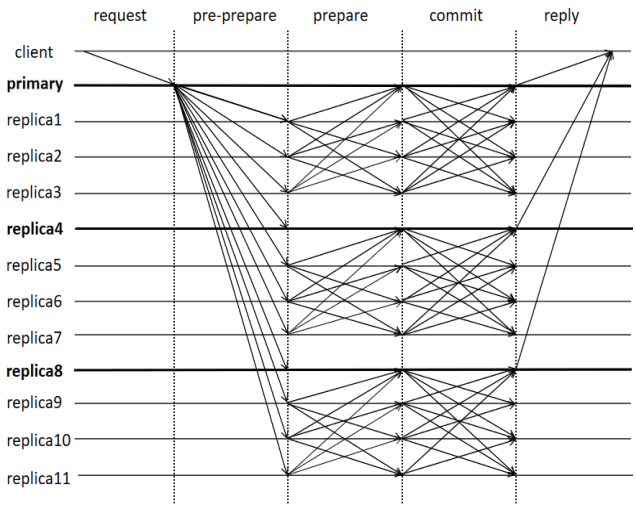

图 2 改进后的 PBFT 算法一致性协议执行流程

3.2 算法流程

3.2.1 客户端操作

客户端将向它认为是主节点的节点发送请求 <REQUEST,

o, *t*, *c* >。这里的 *t* 指的是时间戳，*o* 代表请求的操作，而 *c* 表示的是客户端的详细数据。为了确保每个请求只被执行一次，会在每个请求中添加一个时间戳。这个时间戳记录了请求首次发送的时间，并且每个后续请求的时间戳都会高于第一次发送的请求。这样做的主要目的是防止重复请求对系统造成不必要的负担，同时也能确保数据的一致性和准确性。在返回的结果中，除了包含处理结果本身外，还会附带一个当前视图编号。客户端在接收到返回结果后，会提取出视图编号，并使用它来验证当前的主节点。如果视图编号与客户端之前保存的主节点视图编号一致，就说明当前主节点仍然是之前考虑的主节点，客户端可以放心地向其发送后续请求。

通过这种方式，能够确保每个请求只执行一次，避免了重复请求对系统造成的不必要的负担。同时，通过视图编号的验证和更新机制，系统还能在主节点发生变化时及时调整请求的目标，保证数据的一致性和准确性。

3.2.2 三阶段协议

（1）pre-prepare 阶段

在预准备环节中，主节点主要负责组装预备信息，同时将客户端的请求信息追加在其后 <<PRE-PREPARE, *v, n, d*>, *m*>。*v* 为标识符，表示该消息当前在哪个视图中被编码并发送，*m* 为客户端的请求信息，*n* 是主节点为 *m* 分配的唯一编号，*d* 是 *m* 的摘要信息。

预准备信息获取后，各副本节点将执行同样的程序，来保证预准备信息和客户端的信息完全符合要求，对应的签名均无误，同时验证 *d* 和 *m* 的信息散列是否匹配，还要验证此节点的当前视图是否为 *v*，并确认此节点之前没有收到包含相同视图编号和消息序列号的预准备的消息。预备消息中的序号 *n* 位于低水线 *h* 和高水线 *H* 之间。

（2）prepare 阶段

在准备过程中，将每四个节点作为一个集合，每个集合的第一个节点被选为主节点。该节点负责向其余组内次级节点协调并发布准备信息，同时将预准备及准备信息保存在其信息日志中。准备信息的格式为 <PREPARE, *v, n, d, i*>。在这些节点中，*i* 表示节点的编号，其余参数的意义与预准备信息保持一致。如果所在消息的序列号落在 *h* 和 *H* 的范围内，即视为签名无误，节点将会接收准备信息，并记入消息日志之中。

（3） commit 阶段

在本阶段，副本节点 *i* 将会把确认信息发送给组内其他的所有副本节点，消息格式为 <COMMIT, *v, n*, D(*m*), *i*>。对于副本节点来说，一旦它们收到来自其他节点发出的确认信息，就会检验以下几个要素是否达到了预期的标准：视图的编号是否和现在节点的视图编号一致；签名是否正确无误；是否在 *h* 和 *H* 的范围内请求序列号。一旦满足上述所有条件，节点便会接收确认信息并记录在本地的日志之中。

4 实验结果及分析

4.1 实验设计

该算法的基础是一个需要在多个节点上运行以模拟大量分布式节点的计算的分布式系统，有如下设计。

（1）共识节点：使用进程模拟端口号从 10001 到 20000 的共识节点，共识节点在处理事务和块共识确认时对整个系统至关重要。

（2）交易节点：产生方式是通过进程进行模拟，一个交易节点由每个进程代表，并且每个进程具有不同的端口负责模拟交易数据。每个进程需要以最高速度产生交易信息，并把它们发送到共识节点。

Go 编程语言被应用于构建整个区块链架构，在 Linux 操作系统环境中进行，并利用脚本语言开启多个进程。实验采用了 PBFT 算法标准，对 8、12、16、20、24 个节点进行了基于 PBFT 共识算法优化的性能测试。在这个实验里，每个步骤都按照一定的次序被激活，然后开始运作改进后的 PBFT 算法。根据不同的共识节点的数目，对它们做了 10 轮的独立检查，并将这 10 轮的平均值作为最后的数据成果。

4.2 运行效率分析

目标在于提升区块链运行性能，因此对 PBFT 算法进行了优化。采取 PBFT 算法作为基准，对 4、8、12、16、20 的节点分别进行了 PBFT 算法与优化后 PBFT 算法的时间比对测试。测试结果如图 3 所示。

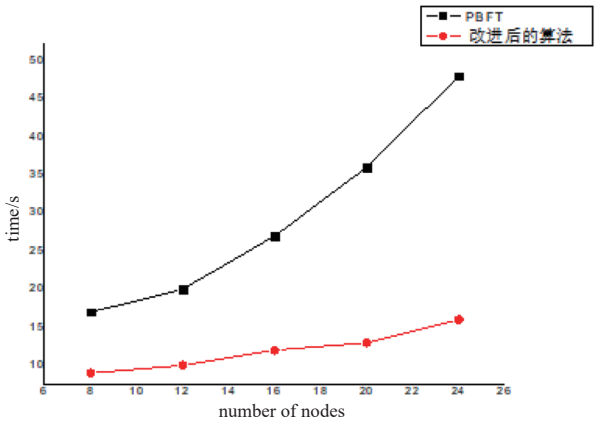

图 3 PBFT 算法与改进后算法的交易时延对比

从图 3 可知，随着共识体系中节点数量不断增加，改进后的 PBFT 算法效率提升越来越明显。

4.3 吞吐量

在区块链中定义上的吞吐量是：

$$TPS = transaction/D_t \quad (1)$$

式中：transaction 指的是在 D_t 期间内，被包装进区块的交易总量。D_t 代表的是从交易传递到区块验证的期间，即块的生成时间。

图 4 是 PBFT 相关算法吞吐量对比图。针对 PBFT 算法与其优化算法，实验统计了处理 1000 条交易的共识时长。通过公式（1）得出吞吐量数据。依据吞吐量曲线图可观察到 PBFT 算法和经过优化算法的吞吐量均与参与共识的节点数呈现出反比关系，即随着节点数量的增加，吞吐量下降。当节点数相同时，原 PBFT 算法的吞吐量明显低于优化后的 PBFT 算法。

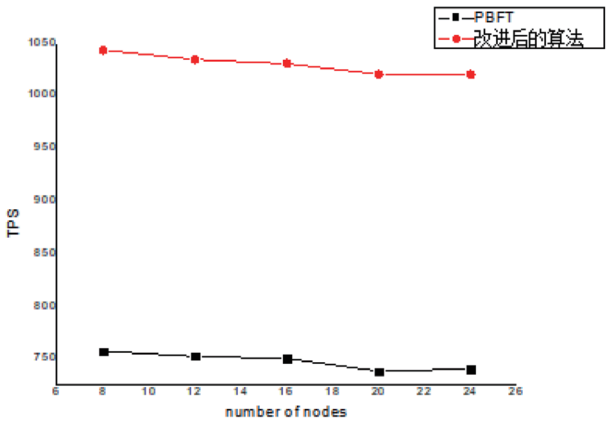

图 4 PBFT 算法与改进后算法的吞吐量对比

4.4 安全性分析

（1）优化 PBFT 算法中根据对节点的编号按顺序进行分组而被选取为主节点，这种选取方式对每个节点被当作主节点具有随机性和公平性。

（2）优化 PBFT 算法的真正目标是将其分解为组内共识，其中共识协议和尝试的替换核心保持不变，并且仍然严格遵守 3*f*+1 原则。

5 总结

针对区块链共识算法中的实用拜占庭容错算法所引发的大量信息广播导致的通信资源过度消耗和低效率问题，提出了新的基于节点分组的共识算法。模拟测试结果显示，改进后的算法很好地解决了 PBFT 算法中的通信资源消耗大和效率低的问题。

参考文献：

[1] 谢卓，张志鸿，李磊，等．基于联盟链的实用拜占庭容错算法的改进 [J]. 计算机科学 ,2022,49(11):360-367.

[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] 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.

[4]LATESH M, SANDHYA A, URMILA S, et al. Block chain for smart systems:computing technologies and applications[M]. Florida:CRC Press,2022.

[5] 高玉龙．区块链的交易安全和隐私保护关键技术研究 [D]. 北京：北京邮电大学 ,2021.

[6] 陈迪．基于区块链的可信域间路由关键技术研究 [D]. 郑州：战略支援部队信息工程大学 ,2021.

[7] 姜臣云．区块链电子数据取证技术应用于知识产权保护的价值分析与路径探索 [C]//《上海法学研究》集刊 2021 年第 21 卷——刑法研究会卷．上海：上海市杨浦区人民检察院第三检察部 ,2021:7.

[8]JUNG J, YOON D, BARRACLOUGH B, et al.Comparison between proton boron fusion therapy (PBFT) and boron neutron capture therapy (BNCT): a monte carlo study[J]. Oncotarget, 2017,8(24):15700.

[9]NGUBO C E, DOHLER M.Wi-Fi-Dependent consensus mechanism for constrained devices using blockchain technology[J].IEEE access,2020,8:143595-143606.

[10] 郭雅菲．基于区块链的数字作品发行权用尽研究 [C]// 世界人工智能大会组委会，上海市法学会．《上海法学研究》集刊（2020 年第 5 卷 总第 29 卷）——2020 世界人工智能大会法治论坛文集．北京：中国政法大学民商经济法学院，2020:15.

[11] 孙建中，田文秀，张琦．基于区块链技术的过程安全管理重点环节的管理及应用 [C]// 中国石油大学（华东），中国化学品安全协会，美国化学工程师协会化工过程安全中心（CCPS）．第六届 CCPS 中国过程安全会议论文集．青岛：赛飞特工程技术集团有限公司 ,2018:11.

[12] 李嘉兴．云计算服务中的区块链技术研究 [D]. 广州：广东工业大学 ,2021.

【作者简介】

吉桐萱（1997—），女，黑龙江大庆人，硕士，研究方向：区块链。

（收稿日期：2024-04-08）