

基于联盟区块链的物流信息平台 LIP-Chain

宁卓¹, 李牧阳²

(1. 南京邮电大学 现代邮政学院、现代邮政研究院, 江苏 南京 210003;
2. 南京邮电大学 物联网学院, 江苏 南京 210003)

摘要:区块链技术是一种基于公钥加密和 P2P 网络的分布式智能账本技术。其去中心化、去信任、信息透明等原生优点完美契合物流行业对数据不可篡改, 信息永久可溯源的需求, 且解决了流通环节多方共同参与情况下的信任问题。但是, 现有主流区块链系统在性能和安全性上难以兼得, 区块链系统中的各项关键技术仍有待进一步改进。针对国内物流快递行业当前发展的痛点, 文中提出了一个基于联盟区块链的物流业信息平台系统 LIP-Chain。该系统解决了传统信息系统中心机构权利过大、信息难以溯源等问题, 重新定义了物流信息的交易和存储方式。对系统设计的关键问题, 如访问控制及身份管理、共识算法、安全与隐私保护等进行了详细分析, 并搭建了原型系统进行仿真实验。实验结果表明, LIP-Chain 不仅吸收了上述区块链技术的特性, 且具有较强的可扩展性, 能够支撑包含上百完整节点以及上千客户端的区块链网络; 资源占用量低, 内存占用不足 100 M, CPU、网络 IO 等开销远低于一般移动设备的硬件配置; 数据吞吐量较大, 可达到每秒几百至几千笔交易。

关键词:区块链; 共识机制; 物流; 信息平台

中图分类号: TP393

文献标识码: A

文章编号: 1673-629X(2019)08-0190-05

doi: 10.3969/j.issn.1673-629X.2019.08.036

LIP-Chain: A Logistics Information Platform Based on Permissioned Blockchain

NING Zhuo¹, LI Mu-yang²

(1. School of Modern Posts & Institute of Modern Posts, Nanjing University of
Posts and Telecommunications, Nanjing 210003, China;

2. School of Internet of Things, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

Abstract: Blockchain is an intelligent distributed ledger technology (DLT) based on public key encryption and P2P networks. Its original advantages, such as decentralization, elimination of trust, and information transparency have perfectly meet the needs of the logistics industry for data not to be tampered with and information to be traceable forever, and solved the problem of trust when multiple parties participate in the circulation. However, the current mainstream blockchain system is difficult to have both performance and security, and the key technologies in the blockchain system still need to be further improved. Aiming at the pain points of the current development of domestic logistics express industry, we propose a logistics information platform system LIP-Chain based on permissioned blockchain. Unlike traditional information systems, LIP-Chain redefines the way to exchange and store logistics data, and solves the centralization and traceability issues perfectly. Furthermore, the key issues are discussed in detail, such as access control and identity management, consensus algorithm, security and privacy protection methods. Finally, the simulation shows that LIP-Chain not only maintains the above merit of blockchain, but also has strong scalability, which can support the blockchain network consisting of hundreds of complete nodes and thousands of clients. With low resource consumption, less than 100 M of memory, CPU, network IO and other costs are much lower than the hardware configuration of general mobile devices. Data throughput is large and can achieve hundreds to thousands of transactions per second.

Key words: blockchain; consensus mechanism; logistics; information platform

收稿日期: 2018-09-24

修回日期: 2019-01-16

网络出版时间: 2019-03-27

基金项目: 江苏省高校自然科学面上项目(16KJB520033)

作者简介: 宁卓(1975-), 女, 博士, 讲师, 研究生导师, 研究方向为网络安全、入侵检测、新一代信息技术在物流中的应用; 李牧阳(1994-), 男, 硕士研究生, 研究方向为区块链关键技术。

网络出版地址: <http://kns.cnki.net/kcms/detail/61.1450.TP.20190327.1629.050.html>

0 引 言

近年来,随着国内电子商务的迅速发展,物流快递行业的业务量迎来了爆发式的增长。但在这种增长背后,隐藏着诸多问题亟待解决。信息溯源难、事故责任含糊不清、企业间数据不流通成为行业现状,传统物流企业的“中心化”管理,使得个体权利过大化,不同企业之间难以互相信任,壁垒由此产生。物流快递业务由众多参与主体构成,核心企业掌握的信息不够对称与透明,并且存在作假的风险,严重影响供应链的管理效率。物流环节区域多、时间跨度长,因此监管困难,假冒伪劣难以根除。

但建设行业级的物流信息平台,实施起来面临着许多困难:物流企业众多,很难信任或支持哪个“龙头”企业创建的行业平台,即去中心化的要求;企业之间既希望通过共享数据互通有无,合作共赢,又不希望泄露自己的关键信息,具有很强的抗大数据分析和数据保密性的要求;既希望发生事故时能通过平台高效溯源,又希望保护快递参与各方的隐私信息;为了提高平台的可信度与权威性,应允许第三方或政府机构的介入监管和审计,平台应具备多方参与特性并保持信息高度透明。

综上,文中提出了一个基于联盟区块链的物流业信息平台系统 LIP-Chain。利用区块链技术的去中心化、数据防篡改、数据溯源三大特性,从底层优化物流行业信息交易与存储方式存在的问题。首先,区块链技术底层由 P2P 网络支撑,所有节点共同维护和验证区块链网络。这种去中心化架构解决了传统系统中中心机构权力过大的问题,非常适合应用于物流快递等需要多方共同参与的业务场景中。其次,区块链交易信息存储在从后向前有序链接起来的区块中。当区块链达到一定长度,区块内的数据在实际上便是无法篡改的^[1]。最后,区块链中大量使用数字签名,并且使用 Merkle 树作为快速归纳和校验完整性的数据结构^[2]。使得数据的溯源、验证、查询流程摆脱传统的人工审计,提高效率的同时大大降低了成本^[3]。配合智能合约,这一特性将在物流业等高吞吐量的交易场景中发挥巨大作用。

除了区块链技术具有的原生性去中心化、去信任、信息不可篡改、易溯源等特点,提出的框架还具有以下优点:

- (1)运行于区块链上的智能合约可在满足条件时自动促成交易,省去了中间环节和大量人工审核成本;
- (2)采用联盟链而非无限制的公有链体制,可在保证去中心化运作的基础上最大限度保护用户隐私和企业机密;
- (3)在区块链网络外层引入身份控制,增强网络

内部信任度,简化验证操作,提升系统效率;

(4)选取了基于拜占庭容错的共识算法 BFT-SMART,在保证性能满足需求的前提下,将系统安全性提升至 33% 拜占庭容错水平。

1 区块链技术研究现状

1.1 区块链数据安全

区块链顾名思义,是由区块组成的链状数据结构。在一条区块链中,区块被从后向前有序地链接,每个区块都指向前一个区块。对每个区块头进行 SHA256 加密哈希^[4],可生成一个哈希值。通过这个哈希值,可以识别出区块链中的对应区块。同时,每一个区块都通过“父区块哈希值”字段引用前一区块(父区块)。这样把每个区块链接到各自父区块的哈希值序列就创建了一条一直可以追溯到第一个区块(创世区块)的链条。

1.2 公有链与联盟链

按照网络中节点拥有的权限公平性,可以将区块链分为公有链、联盟链和私有链三种。文中采用的联盟链机制,适用于对物流快递等对隐私和性能有一定要求的行业^[5]。联盟链的参与者需要通过第三方机构的身份审核,联盟链通过将系统的参与者划分角色,之后赋予不同的节点以不同的权限。

1.3 共识机制

区块链系统中所谓的共识,即所有节点对下一步要将哪些交易数据,以怎样的顺序加入区块链达成一致^[6]。由于区块链系统中存储的交易信息具有实际价值,因此系统内共识的达成不仅是为了性能和稳定性的提升,更直接的原因是为了防止“双重支付攻击”^[7]。

目前的主流共识算法总结见表 1^[8]。

表 1 主流共识算法比较

属性	共识算法					
	PoW	PoS	DPoS	PBFT	RAFT	PoW
拜占庭容错/%	50	50	50	33	0	50
冲突容错/%	50	50	50	33	50	50
区块确认速度/s	>100	>100	<100	<10	<10	>100
吞吐量(TPS)	<10	<1 000	<1 000	<2 000	>10 k	<10
可扩展性	强	强	强	弱	弱	强

综上所述,POW 等概率共识算法为了保证系统的安全性而牺牲了确认速度与吞吐量等其他指标,且这类算法往往需要高性能的节点来支持其复杂的逻辑,不适用于物流行业的交易场景。而 RAFT、PAXOS^[9]等算法只支持冲突容错,一旦系统内出现恶意节点,则有可能因为单一节点导致整个系统崩溃。近年来逐渐

受到关注的拜占庭共识算法^[10]在各项性能上中和了以上两类算法的优缺点,该类算法拥有 33% 的拜占庭容错与冲突容错能力^[11]。根据实际传输的数据不同,交易确认时间一般在几百毫秒至几秒之间,且可以保证 1 000 tps 左右的系统吞吐量。近年来,以 Hyperledger^[12]为代表的企业级、联盟区块链系统也都选择基于拜占庭共识算法作为其下一步发展与研究的方向。

2 LIP-Chain 设计

文中设计了基于联盟区块链的物流业信息平台 LIP-Chain。该设计主要针对以下关键问题进行研究和探讨:系统内的访问控制及身份管理问题;系统内用户和交易数据的安全与隐私保护问题;区块链网络中使用的共识算法问题。

该系统采用联盟链架构,在外层引入 PKI 体系,以此达到强化系统身份管理与访问控制的目的。同时,引入了基于拜占庭容错的 BFT-SMART 协议作为共识算法,在保证系统性能满足实际需求的前提下,将现有联盟链系统普遍采用的冲突容错类共识算法提升至可容忍 33% 拜占庭错误的水平。该系统虽然抛弃了传统区块链完全去中心化的特性,但可以满足行业级信息平台的需求。相反,基于联盟链的多中心化架构有利于充分发挥区块链技术在数据不可篡改、易溯源,多方验证维护等其他特性上的优势,提升了系统的性能与效率。

2.1 系统整体架构设计

提出的系统架构如图 1 所示,整个系统分为两层:应用交互层和区块链共识层。

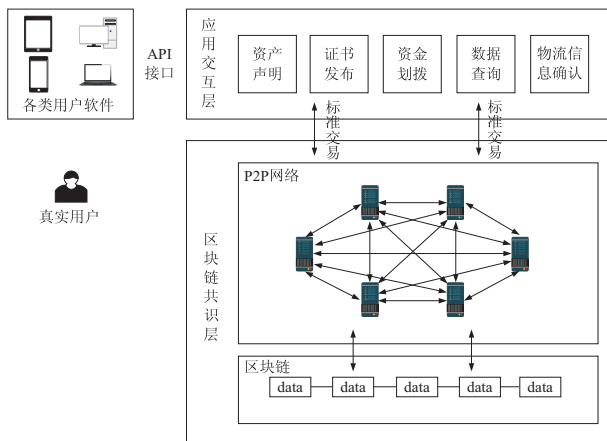


图 1 系统整体架构

应用交互层负责将用户数据和操作封装成符合标准的数字资产,之后以预先定义好的标准交易形式向区块链节点发送各类请求以完成用户操作,并最终将数据存储在区块链上。

区块链共识层包括维护区块链的 P2P 节点网络

和由系统中节点共同维护的唯一一条区块链。主要参与者负责运行作为节点的实体服务器,验证来自上层的交易并将交易组成区块,运行共识算法并最终更新各节点区块链副本中的数据。

2.2 底层 P2P 网络构成

该系统采用模块化设计,将 P2P 网络中的节点分为三种角色:

(1)背书节点:背书节点负责验证交易合法性并对其签名,验证通过后负责执行交易。

(2)组织节点:组织节点接收由背书节点签名完成的交易,运行共识算法,确保一致性后将交易组织成区块后交付给提交节点。

(3)提交节点:提交节点验证组织完成的区块,之后用该区块更新区块链。

2.3 系统交易流程

在设计系统中,一次标准的交易流程由交易背书、生成区块、确认提交三个阶段构成。具体流程简述如下:

客户端向任一合法背书节点发送请求,开始一次交易。背书节点模拟执行该交易的智能合约并读取当前区块链的状态,一并签名后返回给客户端程序。客户端程序接收到数据后,将其与原始交易数据一同打包,广播给所有组织节点。组织节点集群执行基于 BFT-SMART 的改进共识算法,在接收到一定数量的交易或达到一定时间后,将已通过共识算法的交易组织成为一个区块。

每当一个区块完成,组织节点向所有的提交节点广播此区块。提交节点对区块进行时效性与合法性验证,通过后使用区块中的交易数据更新本地的区块链副本。最后,所有提交节点单独通知客户端此次交易是否提交成功。一次完整交易流程结束。

2.4 安全和隐私问题

该系统在数据存储和系统访问控制两个层面保证了交易数据和用户信息的安全。其中在数据存储层面采用中本聪提出的经典区块链结构^[2]。系统内产生的所有数据均被封装在各类标准交易中,由组织节点定期打包为区块后,最终被放入该交易网络所拥有的唯一区块链内,成为区块链不可更改的一部分^[13]。

在系统访问控制层面,该系统引入 X. 509 证书规范^[14]以及 PKI 体系^[15]对系统内身份和权限进行管理。任何加入网络的参与者首先需从证书颁发机构获得数字证书,以作为在网络中活动的唯一合法身份。引入 PKI 体系以密码学原理保证了系统的隐私安全,实现真正的区块链“去信任”。

2.5 共识机制

文中选取了文献[16]提出的 BFT-SMART 算法

应用于该物流业信息平台。BFT-SMART 在拜占庭共识算法的基础上实现了一个模块化的 SMR 协议^[17]。对 BFT-SMART 算法进行了简化,主要修改如下:抛弃了原版算法中的领导人选举操作,客户端将随机选择临近组织节点作为 BFT-SMART 算法中的领导人;在共识算法的任意阶段发生错误后,直接丢弃该交易并通报客户端,而不执行原版 BFT-SMART 算法中的错误处理阶段。

3 仿真实验

3.1 实验环境及配置

为了验证系统设计的可行性,并对系统性能做出评估,文中基于区块链开源框架 Hyperledger Fabric 搭建了底层区块链网络,使用 Fabric SDK 编写应用交互层客户端,执行交易请求。共识机制模块基于文献[18]提供的 BFT-SMART 开源库实现了针对该系统进行改进的 BFT 共识机制。

实验环境配置为: Docker 17.09.0-ce, Hyperledger Fabric v1.1, 在 Mac OS 13.3 上搭建了应用交互层客户端,以及包含 4 个背书节点和 4 个组织节点的底层区块链网络。在 Ubuntu 16.04 搭建了共识机制模块。实验机器为 Macbook Pro17, CPU: Intel Core i5 3.1 GHz, 内存: 16 GB。

为了验证该系统能够满足物流交易场景的实际需求,使用了用户注册和交易信息查询两种标准交易对系统进行了测试,每种交易分别运行 3 000 ~ 5 000 次。通过对相应进程及 Docker 容器进行监测记录,获取了系统吞吐量、交易延迟、节点资源消耗(内存、CPU、网络 IO 占用)几项关键数据。并对改进的共识机制进行了单独测试,得出了其平均共识执行时间。

3.2 实验结果

图 2 显示了在每秒 50、100、150 交易(transaction per second, tps)作为输入的条件下,对系统交易延迟以及输出吞吐量的影响。可以看出,在 50 tps 作为输入的条件下,系统中只需不到 1 s 便可执行一笔交易并

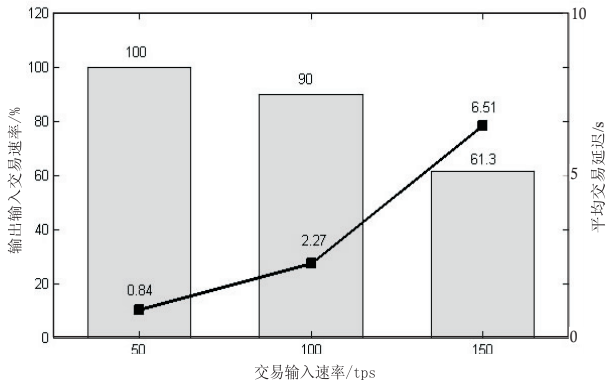


图 2 输入交易速率对交易延迟及输出吞吐量的影响

进行确认,且输出交易速率未受影响。随着输入交易速率的提升,交易确认延迟明显上升,且输出交易速率稳定在 90 tps 左右。

图 3 ~ 图 5 显示了在 50 tps 输入,1 000 笔交易的条件下,各主要进程及容器的资源占用情况。结果表明,1 000 笔交易后,网络流量消耗最高的组织节点约消耗 20 M 流量,系统各主要模块平均 CPU 占用均不高于 20%,各主要模块平均内存占用在 100 ~ 150 M 左右(图中 EP、OP 分别代表背书节点与组织节点)。

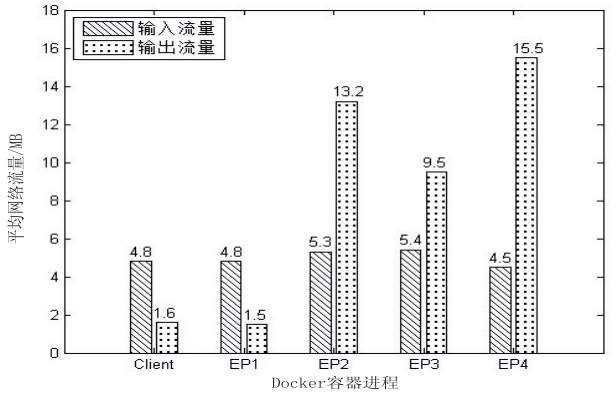


图 3 模拟节点平均网络流量使用情况

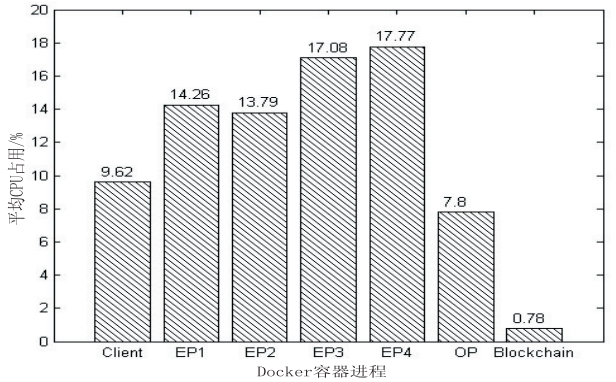


图 4 模拟节点平均 CPU 占用情况

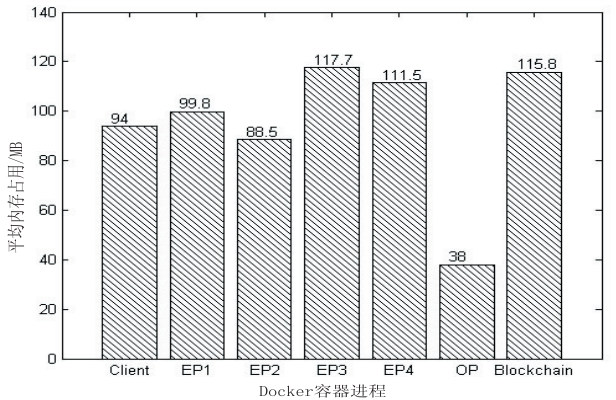


图 5 模拟节点平均内存占用情况

由此可见,该系统各主要模块的资源消耗较低,能适应物流交易业务场景的需求,并应用于手持终端等移动设备。在实际应用场景中,若采取多进程并发处理机制,系统吞吐量有望达到数百甚至上千笔交易每

秒。未来将在这一方向上进行更多研究与验证。

同时,对共识机制模块进行了单独测试。共识模块配置为每区块仅存储一笔交易,收到交易后立即执行后续操作,以此来分析 BFT-SMART 的执行效率。图 6 为在分别使用 1~64 kB 大小的交易进行测试的情况下,基于 BFT-SMART 的共识算法的执行时间。结果显示,单笔交易数据大小在 8 kB 以下时,执行时间较为稳定,超过这一数值,算法执行时间将呈指数级上升。

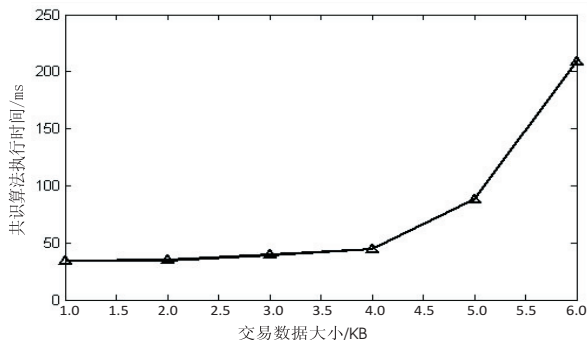


图 6 交易数据大小对共识算法执行时间的影响

4 结束语

针对国内物流行业当前痛点,结合区块链技术优势及特点,提出了一个基于联盟区块链的物流业信息平台。对设计信息平台所涉及的关键问题进行了分析和研究,如访问控制及身份管理、共识算法、安全与隐私保护等问题,并搭建了原型系统进行仿真实验。相比于比特币等加密货币系统以及现有的联盟链系统,该系统具有如下优势:

(1)在区块链网络外层引入 PKI 体系进行身份管理,满足了行业级信息平台对数据透明度与隐私保护机制上的灵活需求;

(2)引入了基于拜占庭容错的 BFT-SMART 协议作为共识算法,在保证系统性能满足实际需求的前提下,将现有联盟链系统普遍采用的冲突容错共识算法提升至可容忍 33% 拜占庭错误的水平;

(3)联盟链架构简化了系统的数据验证与安全机制,交易只需被区块链网络部分节点验证与执行,降低了节点的资源占用需求,节省成本。

该系统虽然在理论上具有一定的研究价值和优势,且仿真结果理想。但要想付诸实践,真正应用于现实交易场景之中,还有许多具体细节需要考虑。下一步的工作是在真实的分布式场景中对系统进行搭建与测试,并对共识算法进行改进。

参考文献:

[1] 袁 勇,王飞跃. 区块链技术发展现状与展望[J]. 自动化

学报,2016,42(4):481-494.

- [2] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[EB/OL]. (2008-11-01)[2018-09-30]. <https://bitcoin.org/bitcoin.pdf>.
- [3] 何 蒲,于 戈,张岩峰,等. 区块链技术与应用前瞻综述[J]. 计算机科学,2017,44(4):1-7.
- [4] 沈 鑫,裴庆祺,刘雪峰. 区块链技术综述[J]. 网络与信息安全学报,2016,2(11):11-20.
- [5] 袁 勇,倪晓春,曾 帅,等. 区块链共识算法的发展现状与展望[J]. 自动化学报,2018,44(11):2011-2022.
- [6] 邵奇峰,金澈清,张 召,等. 区块链技术:架构及进展[J]. 计算机学报,2018,41(5):969-988.
- [7] KARAME G, ANDROULAKI E, CAPKUN S. Two bitcoins at the price of one? double-spending attacks on fast payments in bitcoin[J]. IACR Cryptology ePrint Archive,2012,248(1):1-17.
- [8] PEASE M, SHOSTAK R, LAMPORT L. Reaching agreement in the presence of faults[J]. Journal of the ACM, 1980,27(2):228-234.
- [9] 杨 革,徐 虹. Paxos 算法的研究与改进[J]. 科技创新与应用,2017(7):25-26.
- [10] 张仕将,柴 晶,陈泽华,等. 基于 Gossip 协议的拜占庭共识算法[J]. 计算机科学,2018,45(2):20-24.
- [11] CASTRO M, LISKOV B. Practical Byzantine fault tolerance and proactive recovery[J]. ACM Transactions on Computer Systems,2002,20(4):398-461.
- [12] CACHIN C. Architecture of the hyperledger blockchain fabric[C]//Workshop on distributed cryptocurrencies and consensus ledgers. Switzerland:IBM Research,2016.
- [13] PUTHAL D, MALIK N, MOHANTY S P, et al. The blockchain as a decentralized security framework[J]. IEEE Consumer Electronics Magazine,2018,7(2):18-21.
- [14] HOUSLEY R, FORD W, POLK W, et al. Internet X. 509 public key infrastructure certificate and CRL profile[S]. [s. l.]:[s. n.],1998.
- [15] ADAMS C, LLOYD S. Understanding PKI: concepts, standards, and deployment considerations[M]. [s. l.]:Addison-Wesley Professional,2003.
- [16] BESSANI A, SOUSA J, ALCHIERI E E P. State machine replication for the masses with BFT-SMaRt[C]//44th annual IEEE/IFIP international conference on dependable systems and networks. Atlanta, GA, USA: IEEE, 2014:355-362.
- [17] SOUSA J, BESSANI A. From Byzantine consensus to BFT state machine replication: a latency-optimal transformation[C]//Ninth European on dependable computing conference. Sibiu:IEEE,2012:37-48.
- [18] CRISTIAN F, AGHILI H, STRONG R, et al. Atomic broadcast[J]. Information & Computation, 1995,118(1):158-179.