研究与开发

基于 Fisco-Bcos 平台的区块链系统性能精确分析模型

许鸣睿[1]，姚玉才[2]，朱晓荣[1]
（1. 南京邮电大学，江苏 南京 210003;
2. 南京深业智能化系统工程有限公司，江苏 南京 210018）

摘　要：为了解决区块链系统实际部署面临的性能难以估计、所需的硬件设施性能难以确定等问题，建立了不同网络结构下基于模型和数据融合的区块链网络吞吐量精确表达模型。通过分析实用拜占庭容错（practical Byzantine fault tolerance，PBFT）算法区块链系统的交易流程，综合考虑网络拓扑结构、采用的共识算法、节点的通信方式等状况，基于大量实际数据建立了 Fisco-Bcos 区块链平台的交易吞吐量（transaction per second，TPS）精确表达模型。实际的区块链系统测试结果表明，本文建立的 TPS 预测模型可以在不同的网络结构下保持较高的预测精确度。

关键词：区块链；异构网络；无线通信；TPS 模型
中图分类号：TN915.81
文献标志码：A
doi: 10.11959/j.issn.1000–0801.2023013

A Fisco-Bcos platform based accurate performance analysis model of blockchain system

XU Mingrui[1], YAO Yucai[2], ZHU Xiaorong[1]
1.Nanjing University of Posts and Telecommunications, Nanjing 210003, China
2.Nanjing Shenye Intelligentization System Engineering Co., Ltd., Nanjing 210018, China

Abstract: In order to solve the problems such as difficult to estimate the performance of blockchain system and determine the requirement of hardware facilities, an accurate model of blockchain TPS based on model and data was established under different network structures. Considering the network architecture, the consensus algorithm, the communication of nodes and other elements, the precise model of TPS was established based on the blockchain transaction model of Fisco-Bcos platform and a large amount of actual data fitting. Through the TPS test of the actual blockchain system, the results show that the prediction TPS model established can maintain high prediction accuracy under different network architecture.

Key words: blockchain, heterogeneous network, wireless communication, TPS model

收稿日期：2022–05–29；**修回日期：**2022–12–29
通信作者：朱晓荣，xrzhu@njupt.edu.cn
基金项目：国家自然科学基金资助项目（No.92067101）；江苏省高校“青蓝工程”和江苏省重点研发计划项目（No.BE2021013-3）
Foundation Items: The National Natural Science Foundation of China (No.92067101), Program to Cultivate Middle-aged and Young Science Leaders of Universities of Jiangsu Province and Key Research and Development Plan of Jiangsu Province (No.BE2021013-3)

0 引言

经过多年的发展，物联网应用取得了长足进步。然而，大规模发展物联网仍然面临着一些关键性挑战，特别是建设/运营成本与服务能力之间如何取得平衡的问题。随着智慧城市、共享经济等业务的快速发展，社会对大规模物联网系统的需求一定会进一步扩大，到那时没有任何公司、政府或第三方具有如此庞大的设备认证和信任担保的能力[1]。区块链技术有助于解决物联网跨行业、跨部门、跨网络等服务系统的资源共享、数据安全传输、信用体系构建等方面的问题。近年来，区块链技术成功应用于工业互联网、金融、医疗等领域，可以提供稳定的数据存储服务，确保数据的安全性、可靠性和透明可追溯性。网络中数据的匿名性和加密性极大地保护了用户的隐私[2]。

此外，区块链与未来的 6G 网络结合，通过多接入网络、海量终端、多样化业务、多模资源的协调，可以提高网络的性能和可靠性，可以为网络中的信息交换和价值转移提供可靠的认证机制；同时，区块链可以隐藏和保护网络中的交易敏感内容和用户隐私信息，为对数据隐私有更高要求的应用程序提供定制化的安全服务[3]。因此，区块链可以提升网络的可扩展性、网络间协作能力、安全性和隐私保护能力。然而，差异化的用户需求和不同接入方式等因素的影响，导致目前物联网网络呈现多层、异构的场景，这对区块链网络的性能、部署等提出了挑战，需要在网络的合适位置安置硬件能力足够的区块链节点以保证区块链的性能。

针对上述问题，本文建立了区块链网络主要性能指标交易吞吐量（transaction per second，TPS）与网络环境的模型。分步分析 Fisco-Bcos 区块链平台的交易流程，分别考虑区块链进行交易时通信时间开销和计算时间开销，建立区块链性能和通信、计算资源之间较为精确的模型。并且基于不同的网络结构，模拟区块链交易在网络中广播、执行、共识的流程，探究区块链网络性能和区块链网络结构之间的关系，在考虑区块链网络结构的情况下，总结得到较为精确的区块链性能模型。最后，本文通过搭建实际的网络进行区块链性能测试，以验证本文的区块链性能模型具有良好的区块链 TPS 估算精确度，验证了本文建立的区块链 TPS 性能模型的有效性。

1 区块链性能分析相关工作

现有的区块链性能分析工作大多聚焦于区块链系统本身的吞吐量、错误率等理论信息，很少考虑复杂的网络结构对区块链系统的影响，这导致部署初期对于区块链网络性能的估算难以进行，因此区块链节点部署的硬件需求也难以确定。

近年来，国内外对区块链系统性能评估方面进行了深入研究[4-10]，从不同的角度对区块链的各项性能进行预测或者分析。Abdella 等[4]使用读/写事务时延、读/写事务吞吐量和失败概率等性能指标，对 Ethereum Clique、Ethereum Proof of Work 和 Hyperledger Fabric’s Raft 共 3 个现有系统进行了比较，主要通过实际测试的方式对不同的区块链系统进行了比较，但缺少对实际区块链系统交易流程的分析，因此无法对区块链网络的交易吞吐量做出预测。Jiang 等[5]研究了如何将区块链技术扩展到车联网应用，考虑大数据的分布式和安全存储，提出了一个车联网区块链系统，然后针对该系统的吞吐量进行了详细的理论分析和数值计算，但缺乏实际的区块链网络对理论结果进行验证。Sun 等[6]面向无线区块链网络吞吐量进行了理论分析，考虑时空域泊松分布，推导了信号干扰加噪声比的分布、区块链交易成功率以及整体吞吐量，缺乏实际的测试结果对理论分析模型的支撑。Huang 等[7]提出了分布式网络分裂概率的分析模型，将网络分裂概率表示为网络大小、丢包

率的函数。通过搭建 Raft 区块链网络对模型进行了验证，得出所搭模型可以预测网络分裂时间和分裂概率，面向 Raft 网络的分裂情况做了分析，并通过实践验证了所建立的模型，但对区块链的吞吐量没有做深入的理论分析。Alrubei 等[8]使用基于以太坊授权证明（proof of authority，PoA）的区块链平台进行测试，对蜂窝网络、Wi-Fi 的平均功耗进行性能分析，研究聚焦于网络带宽对稳定性、链上节点同步的影响。文献[9]建立了基于工作量证明（proof of work，PoW）的区块链平台的 TPS 模型，以找出影响区块链共识算法效率的关键因素。文献[10]将各种共识算法分阶段分解，以分析其时间复杂度，包括 PBFT、HotStuff、Raft 等，但没有结合实际区块链的运作方式建立实际区块链的 TPS 模型。

区块链系统交易吞吐量与网络拓扑结构、硬件设备的处理能力、网络状况、应用程序等因素都有着紧密的联系，这导致难以建立精确的 TPS 表达式，目前的研究大部分基于理想的假设模型，缺乏对实际区块链网络运行环境的综合考虑，因此建立区块链网络性能与网络环境之间的模型具有十分重要的理论价值和现实意义。本文结合实际区块链网络的运行环境对区块链的性能进行数值分析，并搭建实际网络验证。

2　系统模型

本文假设网络中具有一定计算能力和存储能力的物联网设备可以被配置为区块链节点，由多个区块链节点构成区块链网络，每个节点具有接收申请、执行交易和存储交易结果等功能。

区块链网络示意图如图 1 所示，区块链节点之间可以通过直接或多跳的方式相互通信，连接到区块链节点的用户设备经过区块链的认证后都可以作为区块链网络的使用者向该区块链网络发出交易申请，节点接收到交易请求后，会对交易进行认证和广播，从而将一条交易添加到区块链各个节点的交易池中。以图 1 中的无线通信系统为例，区块链节点可以作为一个应用程序部署在各级网络设备上，如宏基站、微基站、路由器、个人计算机等，这些设施、设备之间的通信方式不同，而且存在通信速率不高的无线通信，通信情况的复杂性和设备计算能力的不同导致区块链网络的性能难以估算。

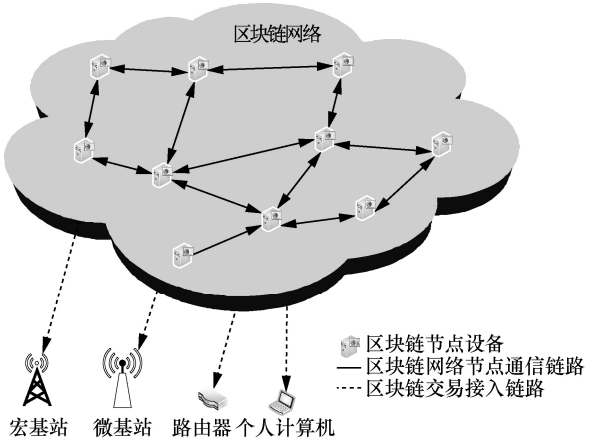


图 1　区块链网络示意图

区块链网络的性能与区块链系统的交易流程、共识方法息息相关，本文基于 Fisco-Bcos 区块链平台进行 TPS 测试。首先分步分析区块链交易时间，并且结合实际的区块链网络结构，拟合成精确的 TPS 估算模型。本文将分析全局耦合网络和随机网络的区块链网络性能，并对不同网络结构进行实际的 TPS 测试，并将测试结果与公式拟合的结果进行比较。

3　基于 Fisco-Bcos 的交易流程分析

3.1　交易流程分步分析

Fisco-Bcos 区块链平台的交易流程包括：交易生成、交易广播、交易打包、交易执行、交易共识以及交易落盘。区块链网络的性能与通信、算力和网络结构息息相关，为了更加精确地构建区块链 TPS 模型，需要对不同的网络结构进行单独分析，首先分步考虑区块链的交易流程，本文涉及的系统参数见表 1。

表 1 系统参数

参数	含义	参数	含义
S_{tx}	每条交易的大小	$S_{blockhead}$	每个区块区块头的大小
C	每个节点的最大传输能力（上行与下行的上限）	$T_{blockdone}$	完成区块内所有交易的时间
N	区块链系统包含的节点总数量	$T_{blockcheck}$	区块验证的时间
$T_{txbuild}$	每条交易构建的时间	T_{tx}	每条交易执行的时间
T_{txsend}	每条交易从客户端发送到区块链节点的时间	S_{result}	区块执行结果的大小
$T_{txcheck}$	每条交易在区块链节点进行验签的时间	$T_{resultsend}$	区块执行结果发送的时间
$T_{blockpk}$	每个区块打包的时间	$T_{consensus}$	交易共识时间
$T_{blocksend}$	每个区块发送的时间	$T_{blocksave}$	交易及执行结果写入硬盘的时间
n	每个区块包含的交易数量		

步骤 1 交易生成，用户发起的交易请求发送到客户端后，客户端会构建一笔有效交易，交易中主要包含发送地址、接收地址、交易内容和交易签名。

由表 2 可知 Fisco-Bcos 区块链平台定义的每条交易包含的身份信息和签名信息大小约为 400 byte。因为交易的内容具有很大的冗余，所以交易在发送前会通过压缩算法对数据进行去冗余化，通过抓包软件测得实际测试中每条交易的平均大小为 50 byte。后续实验中，为了进行区块链 TPS 的共识拟合，在实际的区块链测试中使用相同的智能合约以保证每条交易的大小相同。

那么每条交易由客户端生成并发送到区块链节点的时间为：

$$T_{txbuild} + T_{txsend} = T_{txbuild} + \frac{S_{tx}}{C} \tag{1}$$

其中，$T_{txbuild}$ 是与交易的复杂度和计算机处理速度相关的时间，交易构建的时间相较于通信时间和智能合约的执行时间很短，可以忽略不计。

步骤 2 交易验签，客户端生成的交易被发送到区块链节点后，节点会通过验证交易签名的方式来验证这笔交易是否合法。若这笔交易合法，

表 2 交易内容大小及含义

分组内容	大小	含义
type	enum	指明交易类型
nonce	u256	发送方提供的随机数，交易唯一性标识
receiveAddress	h160	交易接收方地址
gasPrice	u256	本次交易的 gas 的单价
gas	u256	本次交易允许最多消耗 gas 数量
data	vector< byte >	与交易相关的数据，大小与调用的智能合约有关
chainId	u256	记录本次交易所属的链信息
groupId	u256	记录本次交易所属的群组
extraData	vector< byte >	预留字段，若无需求则为空
vrs	SignatureStruct	交易发送方对交易 7 字段 RLP 编码后的哈希值签名生成的数据
hashWith	h256	交易结构所有字段（含签名信息）RLP 编码后的哈希值
sender	h160	交易发送方地址
blockLimit	u256	交易生命周期，该交易最晚被处理的块高
importTime	u256	进入交易池的 UNIX 时间戳
rpcCallback	function	交易出块后 RPC 回调

则节点会进一步检查该交易是否重复，若没有发现重复交易，则将交易加入交易池缓存。若交易不合法或交易重复出现，则将直接丢弃交易。交易验签流程如图 2 所示。

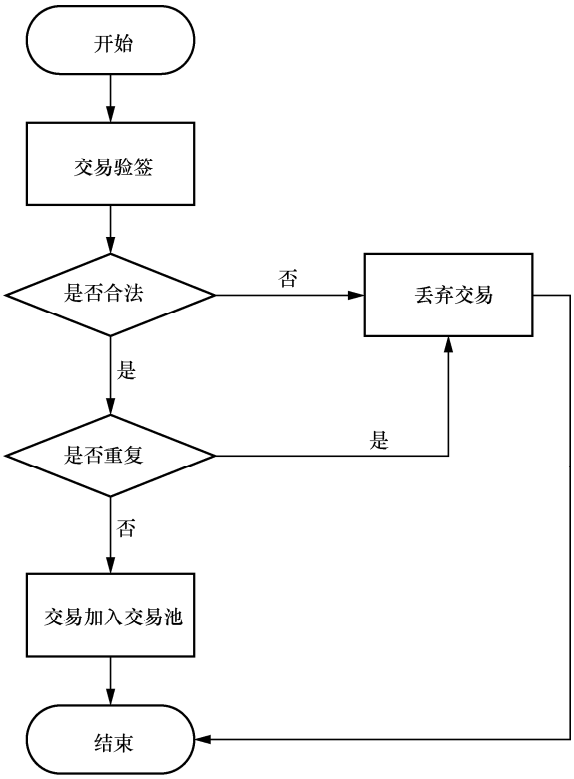


图 2　交易验签流程

步骤 3　交易广播，客户端将交易发送到区块链节点后，当前节点对交易进行验签后，除了将交易缓存在当前节点的交易池外，还会将交易广播至该节点已知的其他区块链节点。每个区块链节点都会对接收的交易进行一次验签，通过验签的交易将会被存入当前节点的交易池。为了方便分析，本文采用的测试交易内容、格式均相同，所以每条交易的验签时间均为 T_{txcheck}，且在交易的总时间中只考虑最晚完成验签节点的验签时间。

步骤 4　交易打包，当交易池中存在未完成的交易时，节点区块打包模块中的 Sealer 线程负责从交易池中按照先进先出的顺序取出一定数量的交易，组装成待共识区块，随后待共识区块会被发往各个节点进行处理，节点将交易打包为区块，如图 3 所示。

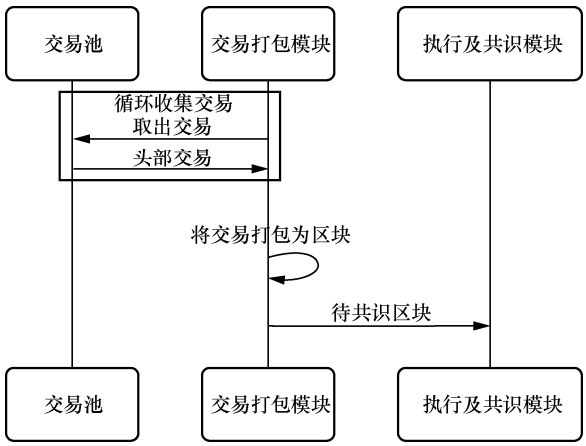


图 3　交易打包流程

交易打包为区块并发送到其他节点的总时间为：

$$T_{\text{blockpk}}+T_{\text{blocksend}}=T_{\text{blockpk}}+\frac{S_{\text{blockhead}}+nS_{\text{tx}}}{C} \tag{2}$$

其中，T_{blockpk} 表示交易在当前节点打包为区块的时间，这与打包区块包含的交易数量以及物理机的处理能力相关。

步骤 5　交易执行，每个区块链节点在收到区块后，首先会对区块的区块头等信息进行验证，区块的合法性通过验证后，当前节点会调用区块验证器把交易从区块中逐一拿出来执行，节点验证区块、交易执行图如图 4 所示。那么每个区块内所有交易完成执行的时间为：

$$T_{\text{blockdone}}=T_{\text{blockcheck}}+nT_{\text{tx}} \tag{3}$$

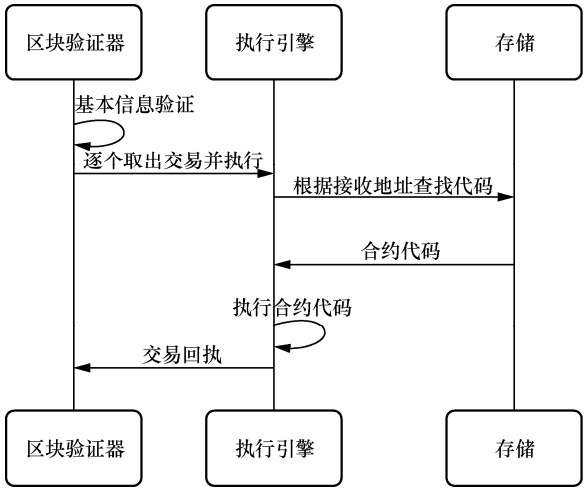


图 4　节点验证区块、交易执行图

步骤 6 交易共识，Fisco-Bcos 中一般采用 PBFT 算法保证整个系统的一致性，各个节点先独立执行相同区块的内容，随后各个节点独立广播各自的执行结果，如果某个节点接收的超过 2/3 的节点都得出相同的执行结果，这说明这个区块在大多数节点上取得了一致，该节点便会开始出块。该过程主要与区块链系统的网络结构相关，这里假设达成共识所需的共识时间为 $T_{\text{consensus}}$。假定区块链网络用矩阵 $\boldsymbol{E}$ 用于记录区块链节点之间的共识情况，如下：

$$\boldsymbol{E}=\begin{Bmatrix} e_{11},e_{12},e_{13}\cdots e_{1N} \\ e_{21},e_{22},e_{23}\cdots e_{2N} \\ e_{31},e_{32},e_{33}\cdots e_{3N} \\ \vdots \\ e_{N1},e_{N2},e_{N3}\cdots e_{NN} \end{Bmatrix} \tag{4}$$

其中，$e_{ij}\in\{0,1\}$，e_{ii} 是节点 i 本地区块的执行情况，若节点 i 已经执行完当前的区块则 $e_{ii}=1$，否则 $e_{ii}=0$。e_{ij} 用于记录节点 i 向节点 j 发送区块的执行结果后节点 j 的验证情况，若结果相同则 $e_{ij}=1$，结果不同则 $e_{ij}=0$。

区块在节点 i 上被认定为合法区块的条件为：

$$\sum_{j=1}^{N}e_{ji}\geqslant\frac{2}{3}N \tag{5}$$

步骤 7 交易落盘，在共识出块后，节点需要将区块中的交易及执行结果写入硬盘永久保存，并更新区块高度与区块哈希的映射表等内容，然后节点会从交易池中剔除已落盘的交易，以开始新一轮的出块流程。用户可以通过交易哈希等信息，在链上的历史数据中查询自己感兴趣的交易数据及回执信息。假设交易落盘所需的时间为 $T_{\text{blocksave}}$。

综上所述，执行完成一个区块的总时间为：

$$\begin{aligned} T_{\text{tot}}=&n(T_{\text{txbuild}}+T_{\text{txsend}}+T_{\text{txcheck}})+T_{\text{blockpk}}+\\ &T_{\text{blocksend}}+T_{\text{blockdone}}+T_{\text{consensus}}+T_{\text{blocksave}} \end{aligned} \tag{6}$$

其中，$n(T_{\text{txbuild}}+T_{\text{txsend}}+T_{\text{txcheck}})$ 为该区块中包含的 n 条交易生成、广播、校验的时间，其余则为区块的打包、广播、执行、共识等时间。Fisco-Bcos 交易完整时序图如图 5 所示。

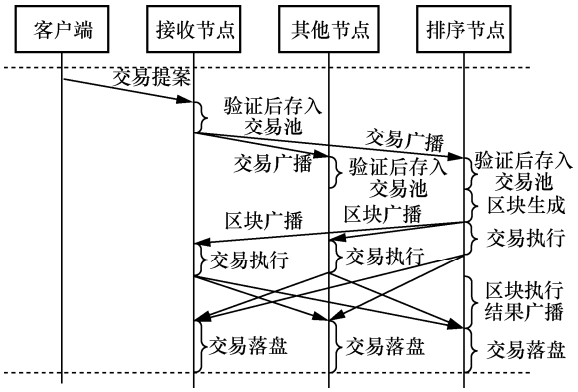


图 5 Fisco-Bcos 交易完整时序图

3.2 视图切换

图 5 中所提到的接收节点、排序节点、其他节点在实际网络中是相同的区块链节点，根据每个节点在一轮交易中承担的任务不同，将节点分为以上 3 种节点。其中，排序节点的任务是按照交易被加入交易池的时间顺序将若干条交易打包为一个区块，同时负责将打包完成的区块发送至区块链的所有其他节点。每一轮负责打包的节点是由 Fisco-Bcos 系统根据视图决定的。PBFT 共识算法使用视图（view）记录每个节点的共识状态，相同视图节点维护相同的 Leader 和 Replicas 节点列表。Fisco-Bcos 系统中，Leader 索引的计算式如下：

$$\text{Leader}_{\text{idx}}=(\text{view}+\text{blockNum})\bmod N \tag{7}$$

其中，view 为一个常数，blockNum 为当前区块链的总区块数量，N 为当前系统包含的节点总数。视图记录了每个节点的共识状态，同时保证了区块共识的正常进行，当 Leader 节点出现故障时，区块链网络将通过视图切换的方式选取出新的 Leader 节点，四节点区块链网络中 Node3 发生故障时的视图切换过程，即 Fisco-Bcos 视图切换如图 6 所示。

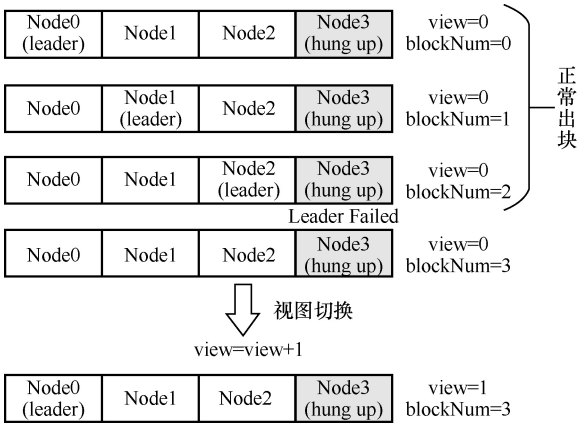


图 6　Fisco-Bcos 视图切换

区块链网络采取视图切换的方式选择共识节点，因此每个节点都有可能成为共识节点进行交易打包和区块广播，不同的节点成为共识节点时区块的广播途径不同，所以对于不同的网络结构来说，需要单独建立一个区块链性能模型。

根据区块链网络的交易流程，TPS 性能与区块链部署的网络结构息息相关，常见的复杂网络模型一般包括 4 种，分别是规则网络、随机网络、小世界网络以及无标度网络。本文主要分析区块链部署在全局耦合网络和随机网络中的 TPS 性能。

4　区块链网络性能分析

本文针对全局耦合网络和随机网络进行区块链 TPS 数学模型的分析，本节将对相应的数学模型搭建实际的网络进行 TPS 测试以验证模型的正确性。

4.1　全局耦合网络 TPS 数学模型

规则网络是网络模型中最简单的网络，典型的规则网络模型主要有 3 种，分别是：全局耦合网络模型、星形耦合网络模型和最近邻耦合网络模型。本文首先分析的区块链网络在物理结构上类似星形耦合网络，星形网络的中心为一个路由器，在逻辑结构上更类似于一个全局耦合网络。

全局耦合网络中任意的两个节点之间都有边直接相连，结构如图 7 所示，全局耦合网络具有最小的平均距离和最大的聚类系数。全局耦合网络假定每个节点的计算和通信能力均相同。

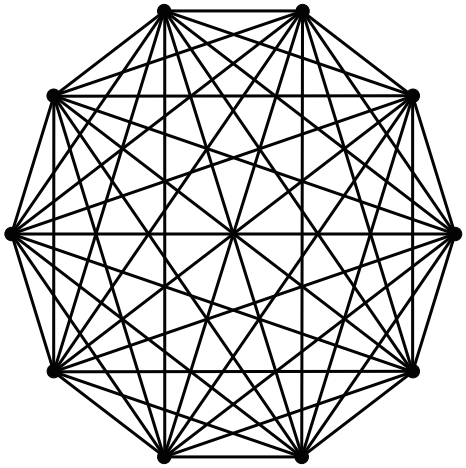


图 7　全局耦合网络结构

在全局耦合网络结构下，任意一个区块链节点与其他节点可以直接访问，并且在交易广播、区块广播和共识阶段只需经过一跳即可到达目标节点。在全局耦合的无线网络中式（6）可以转化为：

$$T_{\text{tot}} = n(T_{\text{txbuild}} + (N-1)T_{\text{txsend}} + T_{\text{txcheck}}) + T_{\text{blockpk}} + (N-1)T_{\text{blocksend}} + T_{\text{blockdone}} + T_{\text{consensus}} + T_{\text{blocksave}} \tag{8}$$

其中，$(N-1)$表示为每个节点广播交易或者区块只需要向网络中其余的节点广播即可，而且与其他节点的通信共享相同的频谱资源，所以所需的交易发送时间和区块广播时间为向一个节点传输的$(N-1)$倍。将前文设定的时间相关参数代入式（8），得到：

$$T_{\text{tot}} = n(T_{\text{txbuild}} + T_{\text{txcheck}}) + n(N-1)\frac{S_{\text{tx}}}{C} + T_{\text{blockpk}} + (N-1)\frac{S_{\text{blockhead}} + nS_{\text{tx}}}{C} + T_{\text{blockcheck}} + nT_{\text{tx}} + T_{\text{blocksave}} \tag{9}$$

式（9）中省去了区块的共识时间$T_{\text{consensus}}$，区块共识中主要耗费时间的过程是区块执行结果的广播，所以$\max\{T_{\text{consensus}}\} = (N-1)\frac{S_{\text{result}}}{C}$，又因为$S_{\text{result}} < S_{\text{tx}}$，且每次广播的区块的大小约为$nS_{\text{tx}}$（本文实际测试中$n \approx 1\,000$），所以$S_{\text{result}} \ll nS_{\text{tx}}$，由此可得$\max\{T_{\text{consensus}}\} = (N-1)\frac{S_{\text{result}}}{C} \ll (N-1)\frac{nS_{\text{tx}}}{C}$，所以在计算通信时间时，$T_{\text{consensus}}$可以忽略不计。

式（9）中包含了区块链系统处理交易的时间，可以将处理交易的时间分成两个部分：通信时间 T_{comm} 和计算时间 T_{comp}，其中通信时间为：

$$T_{\text{comm}} = n(N-1)\frac{S_{\text{tx}}}{C} + (N-1)\frac{S_{\text{blockhead}} + nS_{\text{tx}}}{C} \quad (10)$$

显然，通信时间包含两个部分交易的广播时间和区块的广播时间，其中区块包含区块头和区块体中的交易，而与每个区块包含的上千条交易相比，$S_{\text{blockhead}}$ 远小于 nS_{tx}，所以在计算通信时间时可以将区块头的大小忽略不计。因此将式（10）化简，通信时间 T_{comm} 可以近似为：

$$T_{\text{comm}} = 2n(N-1)\frac{S_{\text{tx}}}{C} \quad (11)$$

除去通信时间式（9）中剩下的均为区块链系统的计算时间，计算式为：

$$\begin{aligned} T_{\text{comp}} &= n(T_{\text{txbuild}} + T_{\text{txcheck}}) + \\ &T_{\text{blockpk}} + T_{\text{blockcheck}} + nT_{\text{tx}} + T_{\text{blocksave}} \end{aligned} \quad (12)$$

可见区块链系统的计算时间包含了交易构建、区块打包、区块校验、交易处理、交易落盘等时间，这些时间与计算机的 CPU 处理能力、内存性能和硬盘性能息息相关，即使确定了硬件的配置，实际运行中处理所需的时间也很难做到精确的定量计算。本文在保证实验环境一致性的情况下，在若干配置相同的计算机上进行单节点的交易处理测试，以求得区块链系统处理交易的平均时间，将该时间作为区块链系统的处理时间。

结合前文中对于全局耦合网络的区块链 TPS 分析，完成一个包含 n 条交易的区块需要的总时间为：

$$T_{\text{blocktot}} = T_{\text{comm}} + T_{\text{comp}} \quad (13)$$

则推导得到全局耦合的区块链网络 TPS 为：

$$\text{TPS} = \frac{n}{T_{\text{blocktot}}} = \frac{1}{2(N-1)\frac{S_{\text{tx}}}{C} + T_{\text{txcomp}}} \quad (14)$$

其中，T_{txcomp} 为每一条交易所需的计算时间，本文通过单节点测试获得；N 为区块链网络的节点总数量；S_{tx} 为每条交易在网络中发送时的实际大小；C 为每个节点的传输速率上限。从式（14）可以看出，每条交易的处理时间近似于交易在全网中广播两次和执行一次的时间和。

4.2 随机网络 TPS 数学模型

与完全规则网络相对应的是完全随机网络，最为经典的完全随机网络模型是 Erdos 和 Renyi 于 20 世纪 50 年代末开始研究的现在称为 ER 随机图的模型[11]，该模型既易于描述又可通过解析方法研究。在 20 世纪的后 40 年中，ER 随机图理论一直是研究复杂网络拓扑的基本理论。

本文研究部署在 ER 随机图网络中的区块链网络 TPS 模型，首先根据 ER 随机图 $G(N, p)$构造算法构造随机网络。ER 随机图 $G(N, p)$构造算法如下。

初始化 给定 N 个节点以及连边概率 $p \in [0,1]$。

随机连边：

步骤 1 选择一对没有边相连的不同节点。

步骤 2 生成一个随机数 $r \in (0,1)$。

步骤 3 如果 $r < p$，那么在这对节点之间添加一条边；否则就不添加边。

步骤 4 重复步骤 1～步骤 3，直至不存在孤立节点且每个节点都被选择过至少一次。

步骤 5 为每条边随机生成一个数据传输速率 $c \in (0, C/N]$。

限制 $c \in (0, C/N]$ 是为了方便之后进行仿真，若假定的带宽超出了实际硬件可以负载的传输速度的上限，则会导致实际传输速率低于仿真中的传输速率。

由第 3.2 节可知，若区块链的所有节点在运行期间均保持正常运行，则区块链系统的主节点将由系统的视图决定，每个节点在测试中将轮流担任区块链的主节点，负责打包和广播区块。而当不同的节点成为主节点时，区块和交易的广播路径将有所不同，由此本文使用算法 1

对不同的节点作为主节点时区块的广播时间进行分析。

算法 1　随机网络区块平均传播时间算法

随机网络的节点数量为 n，随机网络的邻接矩阵 A=[{a_{11}，a_{12}，…，a_{1n}}，{a_{21}，a_{22}，…，a_{2n}}，…，{a_{n1}，a_{n2}，…，a_{nn}}]，每条交易的大小为 S_{tx}，假设每个节点的上行速度上限和下行速度上限为 C；

统计节点的邻居节点数量记为 s={s_1，s_2，…，s_n}；

初始化传播时间矩阵记为 sendtime={t_1，t_2，…，t_n}；

for i=1:1:n

初始化每个节点的到达时间矩阵 arrtime={arr_1，arr_2，…，arr_n}；

$k = i$　　//以节点 i 为主节点

根据算法 2 更新节点到达时间表 arrtime；

t_i = max(arrtime);　//以 i 为主节点到其他节点的最大时间作为当前节点的发送时间

end for

取 sendtime 矩阵的平均值作为当前网络下的广播的平均时间。

算法 2　深度优先传播时间统计算法

随机网络的节点数量为 n，随机网络的邻接矩阵 A=[{a_{11}，a_{12}，…，a_{1n}}，{a_{21}，a_{22}，…，a_{2n}}，…，{a_{n1}，a_{n2}，…，a_{nn}}]，节点的邻居节点数量记为 s={s_1，s_2，…，s_n}，当前到达的节点序号为 k，到达该节点所需的时间为 curT，每条交易的大小为 S_{tx}，假设每个节点的上行速度上限和下行速度上限为 C。

if curT<t_k

arr_k = curT//更新到达当前节点的最短时间；

else

　return　　//已有到达该节点的更短传播路径，结束当前方法；

end if

for i = 1:1:n

　if a_{ki} == 1　//节点 k 和节点 i 之间互通

　curT = curT + S_{tx}/(C / s_k);　　//当前节点可以连通的节点平分传输速度 C，更新下个节点的到达时间

　$k = i$;

　再次调用算法 2，以 i 作为当前节点更新各个节点的到达时间；

　end if

end for

5　模型预测及实验验证

为了验证本文建立模型的有效性，在实验室环境中搭建实际的区块链网络进行 TPS 测试及其他性能分析。实验室搭建区块链网络测试环境使用 5 台计算机作为测试机器，每台计算机使用虚拟机技术分别运行两个 Linux 虚拟机系统，以此来搭建测试环境所需求的 10 节点区块链网络。实验室测试使用的计算机、路由器硬件参数见表 3。

表 3　硬件参数

硬件名称	主要参数
计算机 CPU	I7 6 700 四核八线程，主频为 3.4 GHz
计算机内存	DDR3 16 GB 1 600 MHz
计算机网卡	Intel(R) Ethernet Connection (2) I219-V（1 000 Mbit/s）
虚拟机 CPU	三核三线程（虚拟）
虚拟机内存	DDR3 4 GB 1 600 MHz（虚拟）
虚拟机网卡	虚拟网卡
路由器	Newifi D2 （1 000 Mbit/s）

实验环境搭建的区块链网络测试的主要软件环境见表 4。

表 4　软件环境

软件名称	软件用途/版本
Ubuntu	Linux 操作系统，版本 20.04
Fisco-Bcos	区块链平台，版本 2.8.0
Docker	Docker 容器，版本 20.10.8
Docker-Compose	Docker 容器管理工具，版本 1.25.4
Iperf3	带宽测试工具，版本 2.0.13
wondershaper	Linux 系统下带宽限制工具
Caliper	区块链性能测试工具，版本 0.2.0

5.1 交易计算时间测试

区块链系统的计算时间很难做到精确的定量计算，所以通过在若干配置相同的计算机上进行单节点的交易处理测试，以求得区块链系统处理交易的平均时间，将该时间作为数学模型中每条交易的处理时间。

每条交易的计算时间与交易数量之间的关系如图 8 所示，在单个机器上搭建单节点进行测试，目的是测得较为精确的交易创建、交易执行和交易落盘的总时间。可以看出，每条交易在区块链中生成、验证、执行、落盘的总时间与每次测试输入的交易数量没有明显关系，图 8 中所有交易的平均时间为 0.739 7 ms，下文中将该数值作为区块链处理每条交易的平均时间代入数学模型进行拟合。

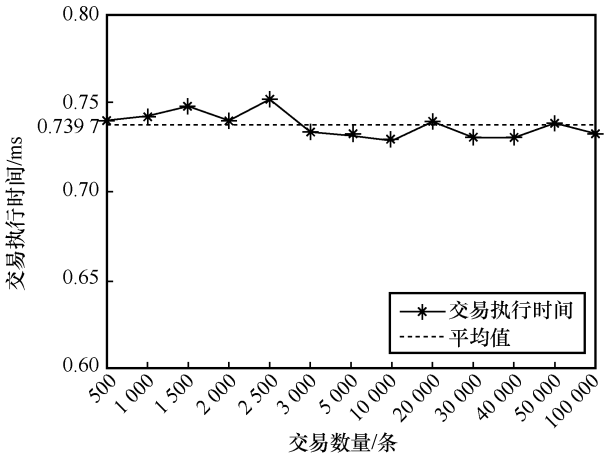


图 8 每条交易的执行时间与交易数量之间的关系

5.2 全局耦合网络模型预测及实验结果

将上文中得到的交易大小 S_{tx}、每条交易的执行时间当作已知量代入数学模型式（14），得到以下针对网络的 TPS 估算曲线：

$$\mathrm{TPS}=\frac{1}{2(N-1)\dfrac{0.05}{C}+0.000\,739\,7} \tag{15}$$

文献[12]中构建的 PBFT 区块链的 TPS 模型如下：

$$\mathrm{TPS}=\frac{\mathrm{Sum}_{\Delta t}(\mathrm{Transactions})}{\Delta t} \tag{16}$$

其中，$\mathrm{Sum}_{\Delta t}(\mathrm{Transactions})$ 表示一个区块包含的交易数量，Δt 表示一个区块生成的时间。

本次实验中参数设定如下：每个区块包含交易数量 n=1 000，节点数量 N（4≤N≤10），每条交易序列化后的数据量大小为 0.05 KB，节点的通信速率变化范围 C（100 KB/s≤C≤40 MB/s）。将本文实验的参数代入式（14），并将式（13）、式（14）中节点的最高通信速率作为自变量进行模型估算，同时搭建实际的全局耦合区块链网络进行 TPS 测试，将本文的模型与文献[12]中的模型进行比较。实验系统中区块链网络拥有 10 个节点，在实验室环境的 Linux 操作系统中部署节点，通过 wondershaper 对节点的上行和下行进行限速，不断改变上下行速率进行 TPS 测试。

10 节点全局耦合网络 TPS 实验结果、本文数学模型理论值对比如图 9 所示，表明本文建立的数学模型和实验室环境中 10 节点全连接区块链系统在通信速率较低的情况下具有较高的精度，在节点的最大通信速率大于 10 MB/s 的情况下出现了较大的误差。误差原因主要是受限于测试环境，实际搭建的区块链系统中使用的千兆路由器最大允许的流量为 100 MB/s，若一个节点的上下行速率高于 10 MB/s 时会在路由器中产生排队发送现象，导致通信效率下降，从而影响实验最终的 TPS 值。从实际测试的 TPS 曲线也能看出在网络带宽来到 10 MB/s 后，节点通信能力的提升对于实际的网络 TPS 几乎没有影响。取图 9 中节点最高通信速率为 50 KB/s～10 MB/s 的数据作为有效数据，可以得到数学模型在全局耦合网络中的最大误差为 6.74%，而文献[12]中理想情况下 TPS 预测的最大误差为 21.5%。因此，本文提出的 TPS 数学模型算法与实际的测试值更接近，具有较高的预测准确性。

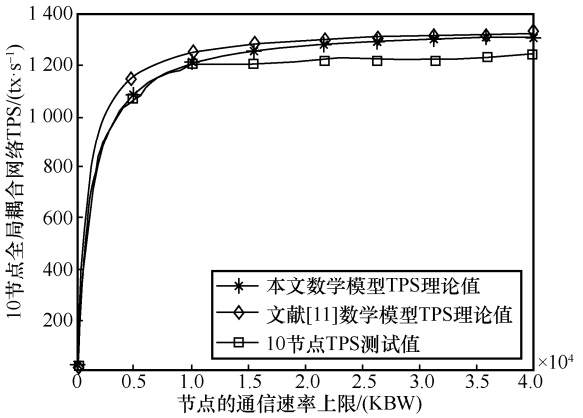


图 9　10 节点全局耦合网络 TPS 实验结果、本文数学模型理论值对比图

5.3　随机网络模型预测及实验结果

根据第 5.2 节中的 ER 随机网络生成算法，ER 算法生成的随机网络如图 10 所示。

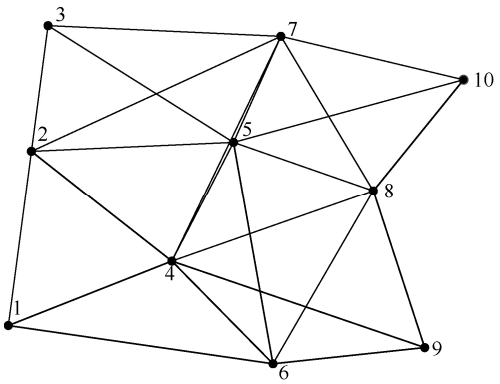


图 10　ER 算法生成的随机网络

将图 10 中的随机网络转化为邻接矩阵作为算法 1 和算法 2 的输入参数，并初始化算法所需的其他参数，即可得到结论：当前随机网络中区块广播的平均时间约为两节点之间单独传输时间的 13.1 倍。将该平均传播时间代入数学模型式（14），即可得到当前的区块链网络 TPS 预测值。

$$\mathrm{TPS}=\frac{1}{2T_{\mathrm{avgcom}}\dfrac{0.05}{C}+0.000\,739\,7} \tag{17}$$

根据图 10 中的随机网络连接情况，在实验室环境中搭建相同的区块链网络图，在修改节点带宽的同时对区块链网络的 TPS 进行测试，10 节点随机网络 TPS 测试值与理论值对比如图 11 所示。

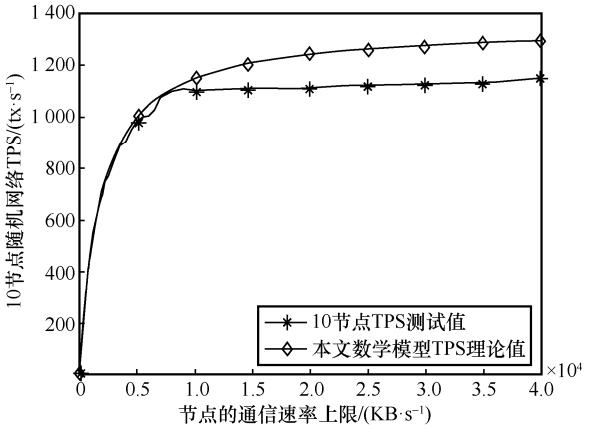


图 11　10 节点随机网络 TPS 测试值与理论值对比

从图 11 中可以看出，建立的数学模型和实验室环境中 10 节点随机网络区块链系统在低速率时具有较高的精度，在节点的最大通信速率大于 10 MB/s 的情况下出现了较大的误差。误差原因主要是受到测试环境的影响。取图 11 中节点最高通信速率为 50 KB/s～10 MB/s 的数据作为有效数据，可以得到数学模型在全局耦合网络中的最大误差为 4.98%。

除了上述 10 节点区块链网络的对比之外，本文对不同的节点数量、网络带宽的网络都做了大量的 TPS 测试与 TPS 理论值对比。不同节点数量和网络状况，预测值和测试值的对比如图 12 所示。节点数量不同时，TPS 预测值与测试值的比较如图 13 所示。

6　结束语

本文对基于 Fisco-Bcos 区块链网络的交易流程进行了分析和研究。考虑区块链网络的实际通信情况和每个节点的通信和计算能力，建立基于 PBFT 区块链系统的 TPS 性能预测模型。并在实验室环境中搭建了相应的区块链网络进行 TPS 测试，以此验证性能预测模型的准确性。预测结果与实际实验结果的对比表明，本文提出的数学模型和预测方法在全局耦合网络和随机网络中具有较高的准确度。

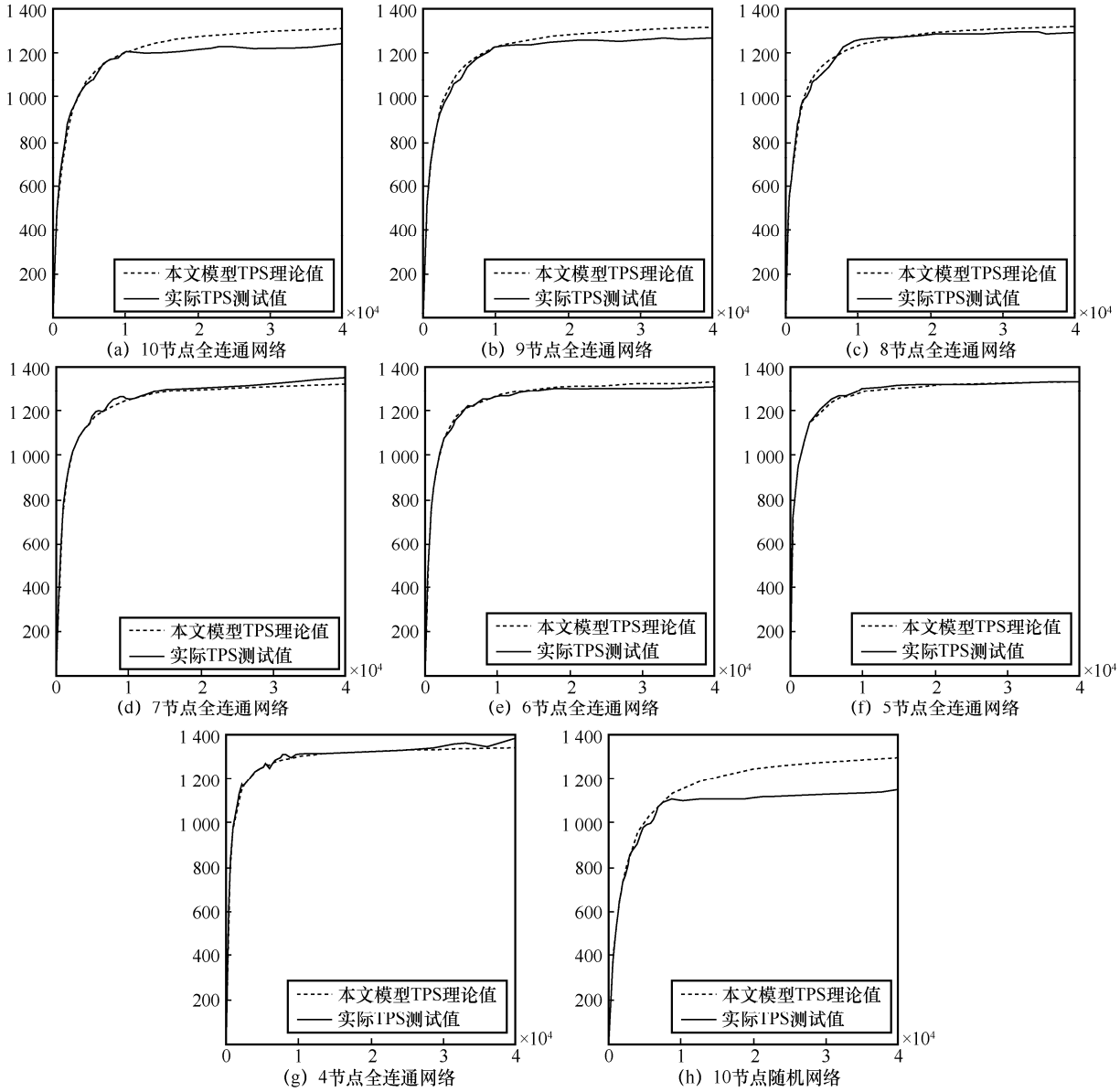


图 12　不同节点数量和网络状况理论值和测试值的对比

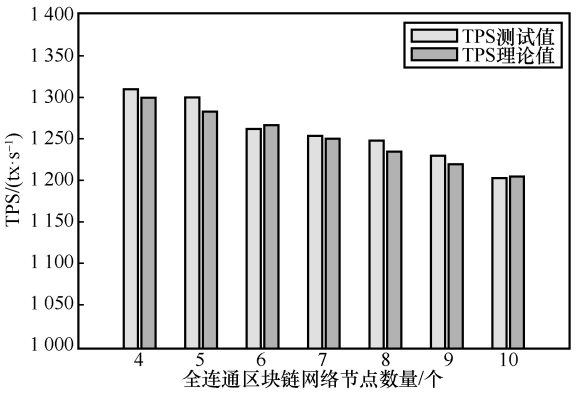


图 13　节点数量不同时，TPS 理论值与测试值的比较

当前区块链技术已经在一些领域取得了长足的发展和应用，例如，杨春燕等[13]将区块链技术应用于电网，提高了电网企业库存管理的效率；刘应等[14]将区块链技术应用于生鲜奶产品溯源，方便问题奶的追踪定位和消费者赔偿，有效改善了生鲜奶行业的溯源现状。但是要将区块链技术真正地大规模落地，必须在实际部署之前能够通过数学模型对实际的区块链性能进行预测，想要搭建区块链系统的组织可以通过本文搭建的 TPS 模型对区块链实际部署

的性能进行估算。为了使区块链技术适用于不同的应用场景，本文建立的数学模型对于不同的区块链应用场景都有一定贡献，如区块链高效的数据查询模型、数据处理优化方案、高效监管制度等。

参考文献：

[1] 巫细波, 杨再高. 智慧城市理念与未来城市发展[J]. 城市发展研究, 2010, 17(11): 56-60, 40.
WU X B, YANG Z G. The concept of smart city and future city development[J]. Urban Studies, 2010, 17(11): 56-60, 40.

[2] 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.
SHAO Q F, JIN C Q, ZHANG Z, et al. Blockchain: architecture and research progress[J]. Chinese Journal of Computers, 2018, 41(5): 969-988.

[3] 代玥玥, 张科, 张彦. 区块链赋能 6G[J]. 物联网学报, 2020, 4(1): 111-120.
DAI Y Y, ZHANG K, ZHANG Y. Blockchain empowered 6G[J]. Chinese Journal on Internet of Things, 2020, 4(1): 111-120.

[4] ABDELLA J, TARI Z, ANWAR A, et al. An architecture and performance evaluation of blockchain-based peer-to-peer energy trading[J]. IEEE Transactions on Smart Grid, 2021, 12(4): 3364-3378.

[5] JIANG T G, FANG H, WANG H G. Blockchain-based Internet of vehicles: distributed network architecture and performance analysis[J]. IEEE Internet of Things Journal, 2019, 6(3): 4640-4649.

[6] SUN Y, ZHANG L, FENG G, et al. Blockchain-enabled wireless Internet of Things: performance analysis and optimal communication node deployment[J]. IEEE Internet of Things Journal, 2019, 6(3): 5791-5802.

[7] HUANG D Y, MA X L, ZHANG S L. Performance analysis of the raft consensus algorithm for private blockchains[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2020, 50(1): 172-181.

[8] ALRUBEI S M, BALL E A, RIGELSFORD J M, et al. Latency and performance analyses of real-world wireless IoT-blockchain application[J]. IEEE Sensors Journal, 2020, 20(13): 7372-7383.

[9] KOKORIS-KOGIAS E, JOVANOVIC P, GASSER L, et al. OmniLedger: a secure, scale-out, decentralized ledger[J]. IACR Cryptology ePrint Archive, 2017: 406.

[10] HU M, SHEN T, MEN J B, et al. CRSM: an effective blockchain consensus resource slicing model for real-time distributed energy trading[J]. IEEE Access, 2020(8): 206876-206887.

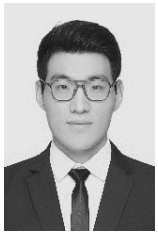
[11] ERDÖS P, RÉNYI A. On the evolution of random graphs[J]. Publication of the Mathematical Institute of the Hungarian Academy of Sciences, 1960(5): 17-61.

[12] WU Y Q, SONG P X, WANG F X. Hybrid consensus algorithm optimization: a mathematical method based on POS and PBFT and its application in blockchain[J]. Mathematical Problems in Engineering, 2020: 7270624.

[13] 杨春燕, 宾冬梅, 黎新. 基于 PBFT 区块链技术的电网企业仓储系统[J]. 电信科学, 2021, 37(2): 144-153.
YANG C Y, BIN D M, LI X. Storage system of power grid enterprise based on PBFT blockchain technology[J]. Telecommunications Science, 2021, 37(2): 144-153.

[14] 刘应, 范洪博, 马首群, 等. 基于区块链的生鲜奶供应链可信追溯系统方案[J]. 电信科学, 2021, 37(5): 148-159.
LIU Y, FAN H B, MA S Q, et al. Blockchain based trusted traceability system scheme for raw milk supply chain[J]. Telecommunications Science, 2021, 37(5): 148-159.

[作者简介]



许鸣睿（1998– ），男，南京邮电大学硕士生，主要研究方向为区块链和联邦学习等。

姚玉才（1975– ），男，南京深业智能化系统工程有限公司副总裁、正高级工程师，主要研究方向为物联网、智慧社区、智慧园区建设等。

朱晓荣（1977– ），女，南京邮电大学通信与信息工程学院教授、博士生导师，主要研究方向为 5G/6G 通信系统、物联网、区块链等关键技术及系统。