基于区块链技术的云制造服务架构及共识算法研究

蒋伟进[1,2,3]，周文颖[1]，李恩[1]，罗田甜[1]，杨莹[1]

（1. 湖南工商大学计算机学院，湖南 长沙 410205；
2. 湖南信息学院计算机科学与工程学院，湖南 长沙 410205；
3. 新零售虚拟现实技术湖南省重点实验室，湖南 长沙 410205）

摘 要：随着信息技术与制造业的深度融合，制造交易网络化成为必然趋势。云制造服务可以实现不受地理空间限制的跨供应商交易，但在交易过程中，存在交易双方的信任难以保障和隐私泄露等问题。为了解决以上问题，提出一种基于双链模式的云制造服务平台架构，将用户数据与交易数据分链存储，并采用实用拜占庭容错（PBFT, practical Byzantine fault tolerance）共识算法解决区块间的数据同步问题。但传统 PBFT 共识算法在存储和共识效率上存在瓶颈，不适合应用于大规模的制造平台上，因此进一步对 PBFT 共识算法展开研究，提出结合 EigenTrust 模型和服务质量（QoS, quality of service）对 PBFT 共识算法进行改进，优化共识集群的选举过程和一致性协议流程，然后给出制造资源寻租和匹配步骤。仿真实验表明，该研究有效提高了 PBFT 共识节点的可靠性，提升了平台的运行效率和区块共识速度，节省了数据存储空间。

关键词：区块链；云制造服务；PBFT；双链模式；服务质量
中图分类号：TP309
文献标志码：A
doi: 10.11959/j.issn.2096−3750.2023.00305

Research on cloud manufacturing service architecture and consensus algorithm based on blockchain technology

JIANG Weijin[1,2,3], ZHOU Wenying[1], LI En[1], LUO Tiantian[1], YANG Ying[1]

1. School of Computer Science, Hunan University of Technology and Business, Changsha 410205, China
2. School of Computer Science and Engineering, Hunan University of Information Technology, Changsha 410205, China
3. Key Laboratory of Hunan Province for New Retail Virtual Reality Technology, Changsha 410205, China

Abstract: With the deep integration of information technology and manufacturing, the networking of manufacturing transactions has become an inevitable trend. Cloud manufacturing services can realize cross-supplier transactions that are not limited by geographical space, but in the process of transaction, there are problems such as difficulty in guaranteeing the trust of both parties and leakage of privacy. In order to solve the above problems, a cloud manufacturing service platform architecture based on a dual-chain model was proposed, which stores user data and transaction data in separate chains, and adopts a practical Byzantine fault tolerance (PBFT) consensus algorithm to solve the problem of data synchronization between blocks. However, traditional PBFT consensus algorithm has bottlenecks in storage and consensus efficiency, and is not suitable for large-scale manufacturing platforms. Therefore, further research on the PBFT consensus algorithm was carried out. The election process was optimized and the consensus protocol process of the consensus cluster was improved by combining the EigenTrust model and the quality of service (QoS), and then give the manufacturing

收稿日期：2022–06–13；**修回日期：**2022–11–20
通信作者：周文颖，zwy1466348907@163.com
基金项目：国家自然科学基金资助项目（No.61772196）；湖南省自然科学基金资助项目（No.2020JJ4249）；湖南省教育厅科学研究项目（No.21A0374）；湖南省研究生科研创新项目（No.CX20221178）
Foundation Items: The National Natural Science Foundation of China (No.61772196), The Natural Science Foundation of Hunan Province (No.2020JJ4249), The Key Scientific Research Project of Education Department of Hunan Province (No.21A0374), The Hunan Provincial Innovation Foundation for Postgraduate (No.CX20221178)

resource rent-seeking and matching steps. Analysis and simulation experiments show that this research effectively improves the reliability of PBFT consensus nodes, improves the operating efficiency of the platform and the speed of block consensus, and saves data storage space.

Key words: block chain, cloud manufacturing service, practical Byzantine fault-tolerant, dual-chain model, quality of service

0 引言

随着信息技术与制造行业的不断发展，制造业对制造方式有了新的要求，即多组件灵活结合、不受空间地域约束、减少资源浪费等，许多制造企业逐渐采取面向服务的网络化制造新模式，以实现制造企业间的协同共生和制造资源的充分利用，加快国家数字产业的创新发展。云制造由李伯虎等[1]提出，它将数字孪生、大数据、物联网以及虚拟化等技术融合在一起，形成一种智能数字化的制造模式。它可以将制造资源和制造能力虚拟成数字化产品，并封装成服务的形式，形成一个遵循一定规则的云制造服务资源池（即制造云）[2]。云制造服务平台可以根据用户的需求，在制造云中组合匹配各类服务，用户选择自己满意的服务后，交易双方签署合约开始服务。目前，互联网中许多巨头企业纷纷实施云制造战略，如海尔、华为、格力、中国核电、美的等。早在 2020 年，云制造服务行业的市场规模就已经较为庞大，在全球约为 569.2 亿美元，在中国约为 1496.5 亿元，而在 2021 年，云制造市场规模更是大幅度增长，为全球制造业经济发展做出了巨大贡献[3]。

云制造服务的出现，为推进制造业务服务化提供了新的解决方案，在有效控制资源囤积带来的额外消耗的同时，降低了制造成本，提升了制造交易的效率和收益。然而，该模式的出现也产生了新的安全隐患。在云制造服务中，几乎所有交易都能在平台上完成，所以其信任安全成为至关重要的问题。同时，在交易的过程中会产生部分隐私信息，因此还存在用户的核心数据被窃取和传播的隐患。另外，传统的云制造服务平台采用的是中心化的管理模式，若中心节点出现故障，将导致整个网络瘫痪。这些缺陷的存在使得云制造服务模式的推广受到了一定程度上的阻碍，成为云制造中亟待解决的关键问题。

自 2008 年中本聪提出比特币，区块链一词随之产生[4]。区块链技术的信息可溯源、数据透明和难以篡改等特点[5-6]，使其可以在没有中心节点监管的情况下，仍能在任意节点间安全地传输信息和进行交易，目前被应用于物联网[7-10]、数字金融[11-14]、工业制造[15-16]、大数据[17-18]、版权保护[19]、商品溯源[20-21]和医疗[22-24]等领域。区块链的一大特点是区块一旦产生难以再被更改，并将一直保留，同时其他节点需要同步更新数据。随着云制造服务平台的持续运行，平台中产生的信息量逐渐庞大，区块链中的区块也随之增加。在区块变多的同时，每个区块需要同步的副本数据容量也在变多，这导致平台存储容量的有效利用率大大降低，大量数据冗余会给平台造成存储膨胀问题，影响区块间共识的速度，制约平台的进一步扩展。

云制造服务中主要有 3 个角色：服务提供者、服务管理者和服务需求者。其中，服务提供者（对应于各企业）需通过认证才有权加入云制造服务平台，这与区块链中联盟链[25]的模式如出一辙。因此，本文将采用适用于联盟链的实用拜占庭容错[26]（PBFT, practical Byzantine fault tolerance）共识算法进行数据同步操作。但 PBFT 共识算法的通信复杂度较高，性能上仍然存在瓶颈。因此，本文针对云制造服务和区块链的结合、PBFT 共识算法的改进开展研究，主要贡献总结如下。

1) 利用区块链技术建立了一种基于双链模式的云制造服务平台架构，设计了用户数据链与交易数据链，将隐私数据与公开数据分开，以提高隐私数据的安全性，减少数据冗余存储空间和数据同步时间。

2) 提出将 EigenTrust 模型和服务质量（QoS, quality of service）相结合，给出了综合信任值和 QoS 综合数值的计算方式，解决了冷启动问题对 QoS 真实性产生的影响，并设计了综合信誉值的计算方式。

3) 针对 PBFT 共识算法的性能缺陷，基于节点的综合信誉值进行共识节点的筛选，选取共识集群中综合信誉值排名第一的节点作为主节点，并简化了一致性协议中的 commit 阶段，减小了共识时延，提高了共识节点的可靠性和交易的执行效率。

1 相关工作

云制造服务的产生，为制造业提供了一种新范

式和新标准，从而引起了众多学者对其进行各方面的研究。Tao 等[27]将云计算、物联网等技术与现有的企业现代制造技术等相结合，形成一种新型的基于计算和服务的云制造模型，对云制造模型的概念、结构、核心技术和特征展开研究。之后，Tao 等[28]又针对云制造的服务组合问题，设计了一种新的并行智能算法，以实现服务组合最优选择。文献[29]采用分布式策略，根据服务平台中服务提供商的决策权，将制造服务分配问题划分成增广拉格朗日协调（ALC, augmented lagrangian coordination）模型，解决了小规模的制造服务分配问题。文献[30]对云制造中的调度问题进行了研究，总结了云制造调度的典型特征和现有不足，给出了解决这些问题的建议。文献[31]研究了云制造场景下的互操作性问题，从云制造服务中提取关键参数，并需要对这些参数进行分析和解释，以此衡量交易是否可行。文献[32]分析了平台、匹配算法和资源对用户效用的影响，提出根据用户的喜好和需求选择不同的算法，以此提高资源的利用率和用户的体验感。为了提高云制造的标准性，文献[33]研究了服务之间的潜在关系，提出了标准制造服务清单的概念，为云制造建立了一种高效的树形服务标准目录，对制造业向云服务的转变起到了很大的促进作用。目前，已有大量学者对云制造服务的资源调度、服务匹配及服务标准等问题进行了相关研究。然而，云制造服务仍然面临着许多挑战，其中，信任问题和数据安全问题严重制约了云制造服务的进一步发展，成为亟待解决的关键问题。

由于区块链多方监管、难以篡改、数据可追溯等特点，在解决分布式管理、信任问题和数据安全方面具有特定的优势，可以在无须信任的情况下安全自主的进行交易、传输数据。同时，区块链还可以实现去中心化的事务处理架构，利用非对称加密和共识算法，在没有第三方监管平台的情况下正确完成交易。因此，一些研究人员将区块链技术与云制造服务集成，用于解决各实体间的信任危机和数据安全问题。文献[34]给出了一种在云生态系统中使用物联网设备的隐私保护方法，能够让实体在不依赖受信任的中心平台的情况下，以匿名的方式证明其制造厂商和调试设备，并且可以在平台中出售设备以获取利益。文献[35]分析了中心化的云制造服务存在的问题，提出了一种基于区块链的对等网络架构，该架构提高了云制造系统的安全性和可扩展性。文献[36]利用区块链存储云制造服务中的服务组合和交易数据，提出了一种 QoS 感知服务组合模型，提高了系统中信息的透明性和去中心化程度。文献[37]将智能合约部署到云制造服务中，提出了一种新型服务水平协议模型，可以有效促使服务提供者和第三方机构提供更好的服务，但其智能合约的部署开销较高。由于云制造平台的交易处于不断的变化之中，文献[38]分析了集中式全局优化模型在云制造中的低效原因，基于区块链技术设计了一个分布式的实时同步平台，便于快速处理平台出现的局部问题。然而，上述文献没有考虑到引入区块链技术后可能出现的数据冗余和存储膨胀问题。区块链具备难以篡改性，因此也无法删除已有区块，当平台不断发展而产生庞大的数据区块时，一方面会占用大量的存储空间，另一方面用户回溯交易信息和节点共识也会花费更多时间，从而影响用户体验感。

区块链采取分布式结构，因此必须使用相应的共识算法实现全网节点的数据同步性。比特币系统采用工作量证明[39]（PoW, proof of work）共识算法，通过比较算力达成共识，但要耗费大量电力资源。权益证明[40]（PoS, proof of stake）共识算法解决了 PoW 的电力消耗问题，由于其不需要通过挖矿获取记账权，因此效率比 PoW 高，但 PoS 的去中心化程度低于 PoW。鉴于 PoW 的能源消耗问题和 PoS 的去中心化程度不足问题，在 Fabric v0.6.0[41]中，PBFT 共识算法被实现，该算法具有一定的容错率，但其通信复杂度较高，共识节点的筛选方式过于随意导致其安全性不足，从而影响共识效率。因此，不少学者对 PBFT 共识算法进行了改进。文献[42]设计了一种多主节点 PBFT（MPBFT, multi-primary node PBFT）共识算法，采用批量共识的方式，增加了 PBFT 共识过程中主节点的可信度，降低了共识所需的时间，但其验证群组仍然采用随机模式，可靠性仍有待验证。文献[43]基于 PBFT 共识算法提出了一种可扩展的双层共识机制，限制了组内的通信，因此通信复杂度有所降低，但同时也影响了通信的实时性，不适合应用于实时交易系统。文献[44]建立了计算节点信誉的模型，共识节点的话语权由其信誉值决定，并且在 PBFT 共识算法的一致性协议流程中扩展了 pre-commit 阶段，其区块链系统的运行效率有所提高。文献[45]通过聚类方法随机选取 k 个代理中心作为共识节点，共识节点轮流当选主节点，且在共识过程中主节点只需要将消息发给

代理节点，提高了区块链达成共识的效率，但由于主节点是轮流当选的，其顺序是固定的，容易遭到恶意攻击。以上研究为解决 PBFT 共识算法的性能瓶颈提供了一定的参考价值，但对于云制造这种需要综合考虑节点可信性和服务能力的平台而言，难以直接应用以上方案。因此，还需要针对制造服务交易的特点，充分考虑节点的信誉情况，提升交易双方的信任度和交易成功率。

2　基于双链模式的云制造服务平台架构

鉴于以往的云制造服务平台网络中心化、用户之间缺乏信任、服务交易质量难以保证、交易过程不够透明等缺陷，本节提出一种基于双链模式的云制造服务平台架构，对传统的中心化云制造服务平台做分布式处理。一方面，利用区块链特有的数据难以篡改性和可追溯性等特点，能够更好的保护平台的数据安全；另一方面，利用双链结构，能够提高平台的运行效率和可扩展性。

根据节点进入区块链系统的方式，可以将区块链分成公有链、联盟链和私有链。其中，节点要想加入联盟链，首先必须进行身份验证并获得相应权限，这种方式加强了区块链系统的安全性，因此，本文采用联盟链构建云制造服务架构。现实中的各个服务提供者在加入云制造服务平台时，需要提交可以证明自己身份的材料，验证通过后方可在平台上发布自己的资源。服务需求者加入平台时同样需要进行身份验证，验证通过后才可以在平台上发布自己的需求，并选择自己想要的服务。

由于在云制造服务中，某些个人信息属于隐私数据，若被他人获取，可能会对用户造成极大的安全威胁，所以应对这类数据采取一定的保护手段。然而，平台中的制造服务交易信息属于公开数据，可以被用户访问以便查看交易进度和交易内容，确保交易按质按量的如期完成。因此本文基于云制造服务中的数据隐私级别，将区块链技术引入云制造服务平台，设计了基于“用户数据链”和“交易数据链”双链模式的云制造服务平台架构，如图 1 所示。

其中，“用户数据链”采用默克尔树结构，用于存放用户信息相对应的唯一 Hash 值，以保证各主体个人信息的真实性和保密性；“交易数据链”采用默克尔帕特里夏树结构，以 key-value 键值对的格式存放数据，因此用户可以快速查找交易数据。这样设计的好处有包括：将用户个人信息和交易信息分流，可以减少区块链中节点存储数据的冗余量，有效提高节点进行共识的时间；区别平台中的隐私数据和公开数据，可以在无须清楚服务提供

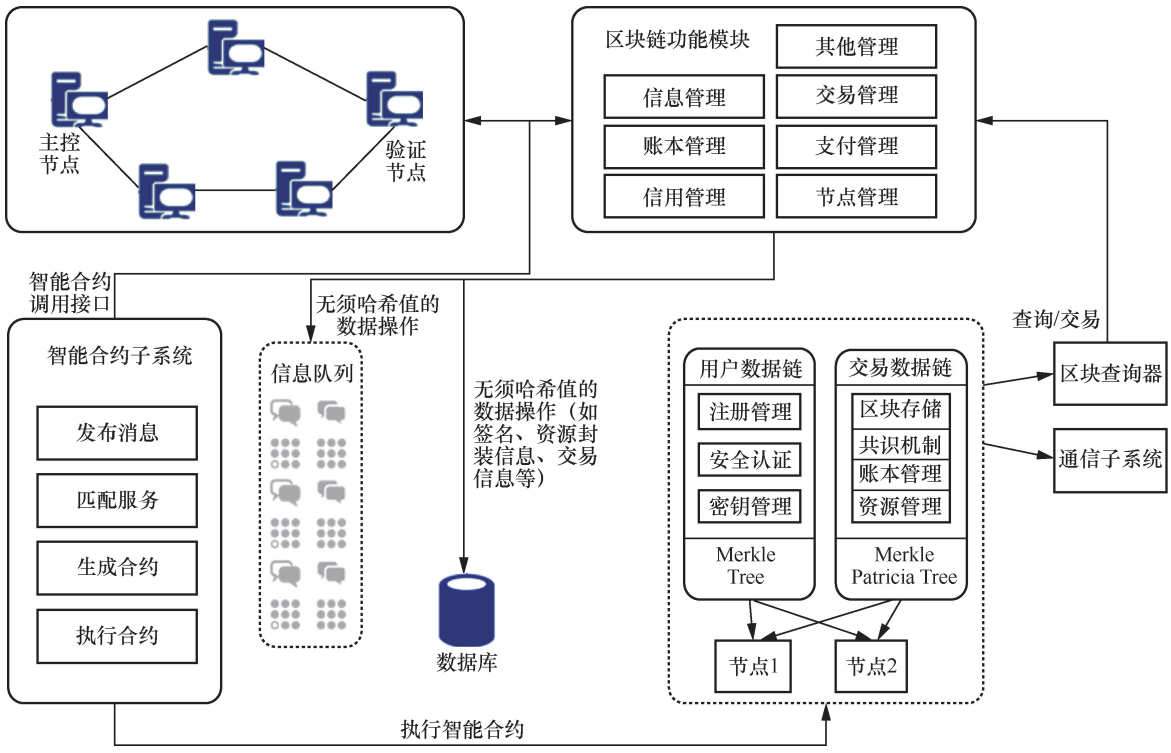


图 1　基于双链模式的云制造服务平台架构

者某些个人隐私信息的情况下，查询平台上的制造资源信息；便于日后与其他平台或机构的业务合作，提升平台的可扩展性与灵活性。

3　基于 EigenTrust 和 QoS 的 PBFT 共识算法

本文采用联盟链模式，因此在共识算法的选择上，本节将采用联盟链中常用的 PBFT 共识算法。PBFT 共识算法用于解决分布式系统中的拜占庭问题，主要分为共识节点筛选和一致性协议两部分[46]。共识节点的筛选是为了建立共识集群，而一致性协议是利用共识节点执行共识算法。在传统的 PBFT 共识算法中，所有节点都需要参与共识，需要耗费大量算力在共识操作上，并且选择主节点的方式存在过大的随机性，所产生的主节点可靠性不高，可能为恶意节点。

EigenTrust 模型是 2003 年由 Kamvar 等[47]提出的，原是用于解决对等网络（P2P, peer-to-peer）中 Peer 实体对行为不负责的问题，但其信任值依据实体间的评分，具有一定的主观性。在云制造服务中，QoS[48]可以用来标识一个服务提供商的服务能力，它包含了服务的吞吐量、服务成本、响应时间、成功率等，可以根据 QoS 值了解企业的制造能力，QoS 值越高则服务水平越好。因此本节先利用 EigenTrust 模型计算各节点的综合信任值，为使服务提供商的综合信誉具有客观性，设计了 QoS 综合评估方式，然后结合 QoS 综合数值和综合信任值得出综合信誉值，以综合信誉值作为选取共识集群的依据，最后优化了 PBFT 共识算法的一致性协议流程。

3.1　基于 EigenTrust 的综合信任值计算

EigenTrust 是 P2P 中常见的一种信任值计算模型，其根据网络中产生的历史交易记录和实体间的评分，有效评估各实体的信任值。从网络结构上来看，区块链就是一种 P2P 模式，因此可以利用 EigenTrust 计算区块链系统中各节点的信任值，以便用户选择更可信的服务商。

首先，对云制造系统中所有的节点进行分类，将与节点 i 有交易的节点划分到 hasTX 集合，与节点 i 无交易的节点划分到 nonTX 集合，然后计算两个节点间的直接信任值（即节点 i 与节点有直接交易）或间接信任值（即节点 i 与节点 j 无直接交易），最后计算出节点 i 的综合信任值。

1) 节点分类

根据节点 i 的历史交易记录，将与节点 i 有过交易的节点划分至 hasTX 集合，与节点 i 没有交易的节点划分至 nonTX 集合。

2) 直接信任值和间接信任值计算

定义 $\mathrm{TX}_{ij}=\mathrm{sat}(i,j)-\mathrm{unsat}(i,j)$，其中 $\mathrm{sat}(i,j)$ 表示节点 i 和节点 j 之间完成的满意的交易数量，$\mathrm{unsat}(i,j)$ 表示节点 i 和节点 j 之间完成的不满意的交易数量。节点 i 和节点 j 之间的直接信任值 C_{ij} 为

$$C_{ij}=\begin{cases}\dfrac{\max(\mathrm{TX}_{ij},0)}{\sum\limits_k \max(\mathrm{TX}_{ik},0)}, \sum\limits_k \max(\mathrm{TX}_{ik},0)\neq 0\\ \dfrac{1}{N}, \text{其他}\end{cases} \tag{1}$$

其中，k 的取值范围为节点 i 的 hasTX 集合中的所有节点。当 $\sum\limits_k \max\left(TX_{ik},0\right)$ 为 0 时，分式无意义，此时设置 $C_{ij}=\dfrac{1}{N}$，N 为系统中的节点数。直接信任值算法见算法 1。

算法 1　直接信任值

输入：节点 node_i、node_i 的 hasTX 集合、节点总数 N

输出：直接信任值 C_{ij}

```
for node_j ∈ hasTX do
    TX_ij = sat(i, j) − unsat(i, j)
    sum = Σ max(TX_ij, 0)
end for
if sum=0 then
    C_ij=1/N
else
    for node_j ∈ hasTX do
        C_ij = max(TX_ij, 0) / sum
    end for
end if
```

在日常生活中，如果想要了解一个人，往往可以通过询问认识这个人的朋友的方式。在云制造系统中，也可以通过这个方式计算彼此之间没有直接交易的信任值，其间接信任值 C_{ij} 为

$$C_{ij}=\sum_m C_{im}\,C_{mj} \tag{2}$$

其中，m 代表与节点 i 和节点 j 都有直接交易的节点。间接信任值算法见算法 2。

算法 2　间接信任值

输入：节点 node_i、node_i 的 nonTX 集合、所有

节点的 hasTX 集合

输出：间接信任值 C_{ij}

查询 node$_i$ 与 node$_j$ 之间的交易路径

for node$_j$∈nonTX do

if node$_m$∈node$_i$ 的 hasTX and node$_m$∈node$_j$ 的 hasTX then

$$C_{ij}=\sum_{m}C_{im}C_{mj}$$

else

迭代计算 C_{ij}

end if

end for

3) 综合信任值

由于某些经验不足或是在线下就有友好关系的节点会对节点 i 给予比实际情况更好的评价，因此需要考虑其他节点自身的综合信任值，其节点 i 的综合信任值 TR$_i$ 为

$$\mathrm{TR}_i=C_{1i}\mathrm{TR}_1+C_{2i}\mathrm{TR}_2+\cdots+C_{ni}\mathrm{TR}_n \tag{3}$$

其中，C_{ni} 代表节点 n 与节点 i 之间的直接或间接信任值，TR$_n$ 代表节点 n 自身的综合信任值。综合信任值算法见算法 3。

算法 3 综合信任值

输入：节点 node$_i$、节点集合 Nodes

输出：综合信任值 C_{ij}

$\mathrm{TR}_i=0$

for node$_j$∈Nodes do

$\mathrm{TR}_i+=C_{ji}\mathrm{TR}_j$

end for

3.2 QoS 指标的综合评估方式

在冷启动阶段，制造服务的 QoS 值由服务提供者设置，后续则通过历史交易记录得出。传统的云制造服务由中心平台统一管理，其 QoS 值存在被中心平台修改的风险，因此真实性有待考验。而在区块链技术中，所有区块一旦产生将难以再更改和删除，其数据具有难以篡改性，因此将 QoS 指标作为评判某制造服务水平的条件有可靠的理论支撑。

QoS 指标分为正指标和负指标，正指标（如吞吐量、成功率）越高，负指标（如服务成本、响应时间）越低，则服务性能越好。由于 QoS 具有多维性，每一维度的指标往往具有不同的量纲，这会对综合评估结果造成一定影响，为了消除各维度的指标之间的量纲影响，需要对其建立一个归一化的计算式。

$$U(ij)=\begin{cases}\dfrac{q_{ij}-Q_j^{\min}}{Q_j^{\max}-Q_j^{\min}}w_j, I(j)=1, i\in(1,N)\\ \dfrac{Q_j^{\max}-q_{ij}}{Q_j^{\max}-Q_j^{\min}}w_j, I(j)=-1, i\in(1,N)\end{cases} \tag{4}$$

$$S_D(i)=\sum_{j=1}^{m}U(ij) \tag{5}$$

如式(4)所示，区块链中共有 N 个节点，$U(ij)$ 表示第 i 个节点的第 j 项 QoS 指标；用一个示性函数 $I(j)$ 表示 QoS 指标的正负性，若 $I(j)$=1，则表示第 j 项指标为正指标，若 $I(j)$=–1，则表示第 j 项指标为负指标；q_{ij} 表示第 i 个节点第 j 项指标的 QoS 值；$Q_j^{\max}$ 表示所有节点中第 j 项指标的最大 QoS 值；$Q_j^{\min}$ 表示所有节点中第 j 项指标的最小 QoS 值；w_j 表示第 j 项指标所占的权重。式(1)用于计算第 i 个节点各项指标的 QoS 值，而式(5)用于将各项指标的 QoS 值加起来，得出第 i 个节点的综合动态 QoS 值。其中，$S_{\mathrm{D}}(i)$ 代表第 i 个节点的综合动态 QoS 值，共有 m 项指标。

然而，在冷启动阶段，QoS 值是服务提供者自己设定的静态数值，初始 QoS 值可能存在主观性过强、设置不合理等问题，因此在计算 QoS 综合数值时，静态 QoS 的权重应当随着服务调动的次数逐渐下降，以此提高总体 QoS 值的可靠性、可用性和真实性。QoS 指标的综合数值计算方法如式(6)。

$$S(i)=\frac{K_i}{K_i+1}S_{\mathrm{D}}(i)+\frac{1}{K_i+1}S_{\mathrm{S}}(i), i\in(1,N) \tag{6}$$

其中，$S(i)$ 表示第 i 个节点的 QoS 总值，$S_{\mathrm{D}}(i)$ 表示第 i 个节点的动态 QoS 值，$S_{\mathrm{S}}(i)$ 表示第 i 个节点的静态 QoS 值，K_i 表示服务调动的次数。

QoS 综合数值的计算过程见算法 4。

算法 4 QoS 综合数值

输入：节点总数 N、QoS 指标的项数 m

输出：QoS 综合数值

for i=0;i<N;i++ do

for j=0;j<m;j++ do

if $I(j)$=1 then

$$U_{ij}=\frac{q_{ij}-Q_j^{\min}}{Q_j^{\max}-Q_j^{\min}}w_j$$

else

$$U_{ij}=\frac{Q_j^{\max}-q_{ij}}{Q_j^{\max}-Q_j^{\min}}w_j$$

end if

end for

$$S_{\mathrm{D}}(i)=\sum U(ij)$$

$$S(i)=\frac{K_i}{K_i+1}S_{\mathrm{D}}(i)+\frac{1}{K_i+1}S_{\mathrm{S}}(i)$$

end for

3.3　共识节点筛选流程

在传统 PBFT 共识算法中，主节点根据式(7)进行选举，这种方式存在较大的随机性，所产生的主节点可能是非法节点，会对系统造成安全危机，因此本节根据第 3.1 节和第 3.2 节中得出的 QoS 综合数值及综合信任值，计算出综合信誉值，其计算方法如式(8)所示。然后，以综合信誉值为基准筛选出共识集群，再从共识集群中选出综合信誉值最高的节点，作为本次共识的主节点，以此确保主节点的可靠性。

$$p=v \bmod |R| \tag{7}$$

其中，p 表示主节点的编号，v 表示视图的编号，$|R|$ 表示节点的数量。

$$\mathrm{Rep}_i=\frac{\mathrm{TR}_i-\mathrm{TR}^{\min}}{\mathrm{TR}^{\max}-\mathrm{TR}^{\min}}+\frac{S(i)-S^{\min}}{S^{\max}-S^{\min}} \tag{8}$$

其中，Rep_i 表示节点 i 的综合信誉值，TR_i 表示节点 i 的综合信任值，$\mathrm{TR}^{\min}$ 表示所有节点的综合信任值中的最小值，$\mathrm{TR}^{\max}$ 表示所有节点的综合信任值中的最大值，$S(i)$ 表示节点 i 的 QoS 综合数值，$S^{\min}$ 表示所有节点的 QoS 综合数值中的最小值，$S^{\max}$ 表示所有节点的 QoS 综合数值中的最大值。

综合信誉值代表该节点既有不错的服务能力，又有较高的服务信用。一般来说，具有较高综合信誉值的节点更可靠。为了提高 PBFT 共识算法的效率和可扩展性，我们可以通过选择一些综合信誉值较高的节点，而不是所有的区块链节点来构建区块链共识集群。一方面，通过排除信誉值较低的节点，可以提高共识的成功率；另一方面，因为共识集群的范围在程度上缩小，可以大幅度减少消息的传递次数，从而提高 PBFT 共识算法的效率。

本文定义一个阈值 $0<\gamma<2$，综合信誉值超过 γ 的节点将被纳入共识集群，筛选出共识集群后，会从集群中选出综合信誉值最高的节点，作为本次共识的主节点。

PBFT 共识集群筛选见算法 5。

算法 5　PBFT 共识集群筛选

输入：节点集合 Nodes、综合信誉值集合 Rep、阈值 γ（$0<\gamma<2$）

输出：共识集群 ConsensusCluster

ConsensusCluster←ϕ

for node$_i$∈Nodes do

if Rep$_i$>γ then

将 node$_i$ 添加到 ConsensusCluster

end if

end for

3.4　一致性协议流程

传统 PBFT 共识算法的一致性协议共分为 5 个阶段：请求（request）、预准备（pre-prepare）、准备（prepare）、确认（commit）和回复（reply）阶段。传统的 PBFT 共识算法一致性协议流程如图 2 所示。

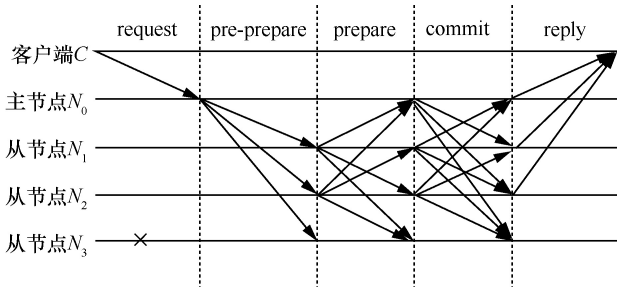


图 2　传统的 PBFT 共识算法一致性协议流程

由于在联盟链中，各节点的加入需要通过相关的身份验证，并且在第 3.3 节中，本文已经基于 QoS 和 EigenTrust 对 PBFT 共识节点的筛选方法进行了改进，共识集群从原本的所有节点缩小到综合信誉值 $\mathrm{Rep}_i>\gamma$ 的节点，主节点由随机产生的方式优化为选取共识集群中综合信誉值最高的节点，具备高信任度和高可靠性。因此，本文优化了 commit 阶段的交互方式，节点无须将确认信息发送至全网节点，只需要发送给主节点，由主节点验证确认结果即可，在一定程度上减少了 PBFT 共识算法的共识时延与共识开销。优化后的 PBFT 共识算法一致性协议流程如图 3 所示。

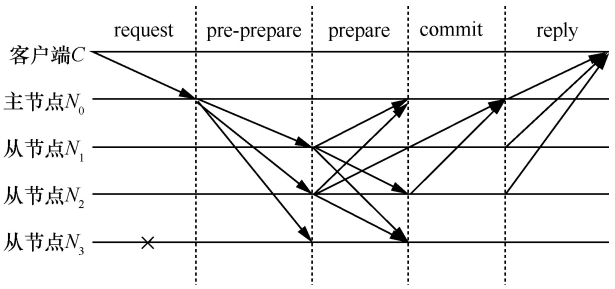


图 3　优化后的 PBFT 共识算法一致性协议流程

假设共识过程中的拜占庭节点数为 f，一致性协议的详细过程如下：

1) request 阶段：客户端 C 将<REQUEST, *o*, *t*, *c*>请求发给主节点 N_0，其中，*o* 代表客户端所发请求的具体动作，*t* 代表此次请求的时间戳，*c* 代表这个客户端的身份，REQUEST 中含有消息内容 *m* 及其摘要 *d*(*m*)。

2) pre-prepare 阶段：主节点 N_0 查验是否为客户端本人的签名，根据请求序号 *n* 对请求消息 *m* 排序并生成 pre-prepare 消息<<PRE-PREPARE, *v*, *n*, *d*> , *m*>，其中，*v* 代表视图的编号，*n* 代表此次请求的序号，*d* 代表消息内容的摘要，*m* 代表消息的具体内容。在此阶段，主节点会将 pre-prepare 消息发送给其他节点。

3) prepare 阶段：从节点验证主节点的 pre-prepare 消息签名，检查当前从节点在当前视图 *v* 下是否已有序号为 *n* 但签名不一致的 pre-prepare 消息、摘要 *d* 与消息 *m* 的摘要内容是否相同、序号 *n* 是否在高低水位内。若查验通过，从节点向其他的所有节点发送 prepare 消息<PREPARE, *v*, *n*, *d*, *i*>，其中，*i* 表示当前节点的身份。从节点对比其他节点发来的 prepare 消息和之前主节点发来的 pre-prepare 消息，若有 $2f+1$ 的节点发来的 prepare 消息与 pre-prepare 消息一致，则完成该阶段。

4) commit 阶段：主节点和从节点验证接收到的 prepare 消息，核实签名和请求 *n* 是否正确、*n* 是否还在高低水位内、摘要 *d* 的内容是否与 pre-prepare 消息中的 *d* 一致。当节点 *i* 收到验证通过的 prepare 消息达到 $2f+1$ 个时，不同于传统 PBFT 共识算法需要向所有共识节点发送 commit 消息<COMMIT, *v*, *n*, *d*, *i*>，这里只需要向主节点发送。

5) reply 阶段：主节点验证从节点发来的 commit 消息的正确性。若有 $f+1$ 个 commit 消息无误，则说明此次共识过程中的大部分共识节点进行了正确的共识操作，则执行具体动作 *o*，将 reply 消息<REPLY, *v*, *t*, *c*, *i*, *r*>发送给客户端，其中，*r* 代表执行具体动作后得到的结果，若客户端得到的一样的 reply 消息达到 $f+1$ 个，则说明此次请求成功。

改进的 PBFT 共识算法一致性协议过程见算法 6。

算法 6 改进的 PBFT 共识算法一致性协议过程

request 阶段：

客户端发起<REQUEST, *o*, *t*, *c*>请求，激活主节点的服务操作

pre-prepare 阶段：

if 请求合法 then

为该请求编号并进行排序

生成 pre-prepare 消息<<PRE-PREPARE, *v*, *n*, *d*> , *m*>

end if

prepare 阶段：

if 从节点接收到的 pre-prepare 消息合法 then

从节点向其他节点（包括主节点）发送 prepare 消息<PREPARE, *v*, *n*, *d*, *i*>

end if

commit 阶段：

for 0<*i*<*C* do

从节点 N_i 检查 prepare 消息是否合法

if 从节点 N_i 接收到 $2f+1$ 个合法的 prepare 消息 then

向主节点发送 commit 消息<COMMIT, *v*, *n*, *d*, *i*>

end if

end for

reply 阶段：

主节点检查 commit 消息是否合法

if 主节点接收到 $f+1$ 个合法的 commit 消息 then

执行本次请求的具体操作

发送 reply 消息<REPLY, *v*, *t*, *c*, *i*, *r*>给客户端

end if

if 客户端收到 $f+1$ 个相同的 reply 消息 then

更新各节点的 QoS 值。

end if

4 制造资源寻租和匹配步骤

假设在云制造服务平台上有一个制造服务需求集 MSD 和一个制造服务供给集 MSS，则基于双链模式的云制造服务平台的可信交易过程如图 4 所示。

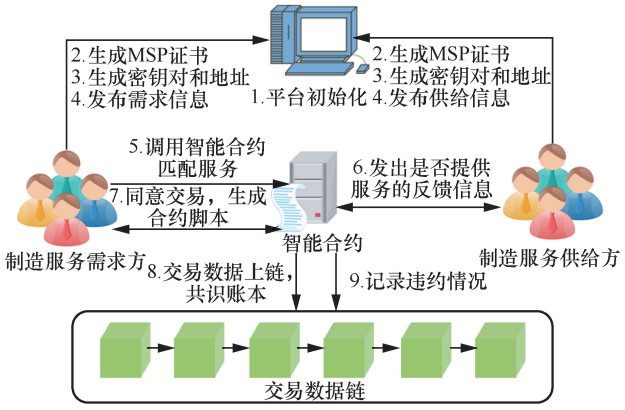


图 4　云制造服务平台的可信交易过程

步骤 1　初始化区块链 BC，如式(9)所示。其中，MSD 是制造服务需求集；MSS 是制造服务供给集；TDC 是交易数据链；UIC 是用户数据链；CA 是共识算法，本文采用第 3 节所提基于 QoS 和 EigenTrust 的 PBFT 共识算法；IC 是智能合约；T 是制造服务需求与制造服务供给的笛卡尔集，T={ti∈MSD×MSS}, ti 为 MSD×MSS 中的一个元素。

$$\mathrm{BC}=(\mathrm{MSD},\mathrm{MSS},\mathrm{TDC},\mathrm{UDC},\mathrm{CA},\mathrm{IC},T) \tag{9}$$

步骤 2　由于本文所提出的云制造服务平台是基于联盟链的形式设计的，因此需要生成自己的成员关系服务提供者（MSP, membership service provider）证书，MSP 不仅可以用于确定哪些身份可以加入该联盟链，还能在交易时进行身份验证和数字签名验证，包含了参与者的公钥和私钥。

步骤 3　msd_i 为制造服务需求集中的某一需求节点，mss_i 为制造服务供给集中的某一供给节点。msd_i 和 mss_i 在这一阶段生成密钥对和地址，后续需要利用密钥对和地址传输信息，并对信息进行加密与解密操作。

步骤 4　msd_i 和 mss_i 在云制造服务平台上发布自己的需求或供给消息，并添加到对应的交易数据链上。$m.\mathrm{msd}_i$ 是 msd_i 在平台上发布的制造服务需求信息，主要包括 msd_i 的地址、制造服务需求量、制造资源类型、制造资源购买预算范围、地理位置、服务时间、响应时间和综合信誉值等；$m.\mathrm{mss}_i$ 是 mss_i 在平台上发布的制造服务供给信息，主要包括 mss_i 的地址、制造服务供给量、制造资源类型、制造服务出售价格、地理位置、服务时间、响应时间和综合信誉值等。

步骤 5　平台根据 msd_i 和 mss_i 的参数信息，在制造服务需求信息上链时调用智能合约为其匹配符合条件的制造资源供给服务，其智能合约采用云制造服务平台的私钥加密，智能合约的内容可以由云制造服务平台给出，也可以由 msd_i 自己设定，从而给予用户更大的自主选择权。

步骤 6　mss_i 根据 msd_i 提供的地址查找公钥，再与 $m.\mathrm{msd}_i$ 中提供的公钥信息比对，以此确认 msd_i 的身份，若身份验证通过且愿意为 msd_i 提供服务，则 mss_i 向 msd_i 回复服务的反馈信息 $r.\mathrm{mss}_i$，然后利用 msd_i 的公钥加密反馈信息，利用 mss_i 的私钥完成数字签名。

步骤 7　当 msd_i 收到反馈信息后，先用自己的私钥解密，得到 mss_i 发送的信息，再根据 mss_i 的地址找到 mss_i 的公钥，利用其公钥对反馈信息中的数字签名解密，以此确认 mss_i 的身份。在 msd_i 确认了 mss_i 的身份，并知晓 mss_i 所提供服务的具体内容后，选择是否接受该需求方的服务，若接受则生成合约脚本，并将交易信息发送至所在链的所有节点，通过第 3 节所提改进后的 PBFT 共识算法对所有节点进行共识操作，更新各节点的账本信息。

步骤 8　双方签订交易合约后，mss_i 则根据合约内容为 msd_i 提供制造服务，在服务期间，区块链将与实际的制造工作及物流系统相结合，制造过程中产生的各类信息将被存放在区块链中相应类别的交易数据链上，并由区块链对其进行审核和监管，确保制造过程透明可见、制造信息不被篡改、制造情况可供追溯，直至整个交易结束为止。

步骤 9　若双方在交易中出现违约情况，平台将自动调用智能合约对违约方进行处罚，其惩罚规则已事先写入智能合约，一旦产生违约行为就会立刻执行违约处罚，并将违约信息广播至所在交易数据链上的所有节点进行同步更新，其将影响到用户的综合信誉值，作为日后筛选共识节点和选择服务的依据，以此提高交易的成功率和可信度。

5　性能分析与仿真实验

本节将从安全性、通信次数、双链模式与单链模式的比较、QoS 指标评估方法、共识时延与吞吐量几方面进行分析与仿真实验。文献[44]与本文一样根据节点的信誉值选取主节点，但其共识节点仍为所有节点，信誉模型也只考虑了共识中的节点表现；文献[45]在 PBFT 共识算法的一致性协议中，与本文类似地通过减少节点发送消息的次数来提高共识效率，但是主节点的选取是依序当选的。综

上，虽然文献[44-45]改进 PBFT 共识算法的出发点与本文类似，但其具体的实施方法有很大的不同。因此，本节将比较本文所改进的 PBFT 共识算法与文献[44-45]的性能。仿真平台为 MATLAB，实验环境为 Intel(R) Core(TM) i5-6300HQ CPU、8 GB 内存、1 TB 硬盘，实验涉及的参数设置有：总节点数为 n，共识集群中共识节点的数量为 C。

5.1 安全性分析

1) 可靠性

本文根据服务提供者的历史记录计算出节点的 EigenTrust 值和 QoS 值，从而得出综合信誉值，以综合信誉值为基准选择共识节点。综合信誉值代表了一个服务提供者的可信性和服务能力，通过选择拥有高综合信誉值的节点参与共识过程，可以有效提高共识节点的安全性。另外，在共识过程中，如果主节点产生了作恶行为，将错误的消息发送给其他节点，非拜占庭节点并不会通过对该消息的验证，若客户端最终收到 f+1 个节点发来的验证不通过的消息，则可以判定主节点作恶，切换视图，更新综合信誉值并重新选举主节点；如果从节点作恶，即某拜占庭节点不通过正确的消息或者篡改消息并验证通过，网络中的拜占庭节点数最多有 f 个，其他 2f+1 个非拜占庭节点不会通过该消息，最终无法被写入区块，同时由于共识过程中产生的数据可以被追溯，所以可以查出作恶节点，作恶节点则可能因此被更换。因此，本文所改进的 PBFT 共识算法可以有效抵制节点的恶意行为，无论是主节点还是从节点作恶，其错误信息都不会加入区块链中。

2) 数据保密性

本文考虑到了用户隐私的问题，采取双链模式将平台中的用户数据与交易数据分开，设计了用户数据链与交易数据链，用户数据链的内容属于隐私内容，在默克尔树中存储的是用户数据对应的 Hash 值，可以满足用户对隐私保护的需求。而交易数据链的内容属于公开信息，每个节点都可查询，方便服务需求者在选择服务时根据历史交易记录分析服务提供者的服务水平。双链模式的设计一方面保证了交易的实时可查询性，为用户追溯交易情况提供便利，另一方面又保护了用户的个人隐私。另外，第 4 节中已经详述过，在交易生成过程中，制造服务需求节点 msd_i 和制造服务提供节点 mss_i 会产生自己的公钥和私钥，通过“公钥加密，私钥解密”的非对称加密方式传输信息，其信息难以被篡改且可以被追溯。

5.2 通信次数分析

原 PBFT 共识算法主要的 3 个阶段中，在 pre-prepare 阶段，主节点需要向全网节点广播一次信息，通信次数为 n–1；在 prepare 阶段，从节点需要向其他节点广播一次信息，通信次数为 (n–1)(n–1)；在 commit 阶段，主节点和从节点都需要向其他节点广播一次信息，通信次数为 n(n–1)。因此，其单次通信总次数为 $2n^2-2n$。

文献[44]简化了 PBFT 共识算法的一致性协议流程，通过增加 pre-commit 阶段来减少 commit 阶段的通信次数，相比于传统 PBFT 共识算法来说，总通信次数减少为 n^2+2n-3。

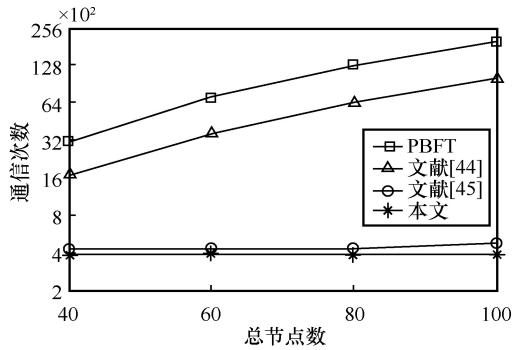
文献[45]利用聚类方法，将全网节点划分成 m 类，每类有 n/m 节点，共识过程分为请求、预备 1、预备 2、准备、确认 1、回复 1、确认 2、回复 2 共 8 个阶段，总通信次数为 $\frac{2n^2}{m^2}+m^2+m$。

本文设置了共识集群，只需要 C 个共识节点进行共识操作，并基于联盟链中节点加入需要进行身份验证的特征，简化了 3 个阶段中的 commit 阶段，将原本所有共识节点都需要进行一次全网广播优化为只需要从节点向主节点发送 commit 消息。因此，本文改进后的 PBFT 共识算法的总通信次数为 C^2-1。

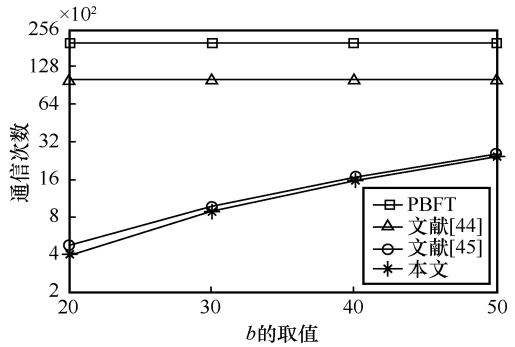
改进后的 PBFT 共识算法的时间复杂度虽然仍为 $O(n^2)$，但其通信次数大大减少。为了更直接的反映上述 4 种 PBFT 共识算法的通信次数的对比，设置参数 n 分别为 40、60、80、100，表示总节点数，b 分别为 20、30、40、50，对于文献[45]而言，b 代表 m，对于本文改进的 PBFT 共识算法而言，b 代表 C，其通信次数对比如图 5 所示。

从图 5 可以看出，b 值固定，总节点数增加时，PBFT 共识算法和文献[44]、文献[45]都是随之增加的，但是对于本文来说，只要 b（即 C，共识集群的数量）不变，通信次数便是恒定的，且比另外 3 种 PBFT 共识算法的通信次数少。当总节点数不变，b 值增加时，传统 PBFT 共识算法和文献[44]是恒定的，因为这两种 PBFT 共识算法的通信次数只与 n 有关，而文献[45]与本文的 PBFT 共识算法的通信次数是随之增加的，且本文的通信次数略低于文献[45]。然而，文献[45]的主节点采取轮流当选的

形式，其可靠性不足，而本文改进后的 PBFT 共识算法依照云制造服务提供者的综合信誉值选举主节点，让每个节点都有机会成为共识节点，但前提是要在历史记录中保持良好行为，增加了共识节点的可信度和平台的稳健性。



（a）b=20，总节点数为40～100



（b）总节点数为100，b为20～50

图 5　通信次数对比

5.3　双链模式与单链模式的比较

区块链主要分为公有链、私有链和联盟链。其中，公有链是完全去中心化的区块链，任何人无须身份认证就可以加入、离开和读写数据。私有链设置了访问权限，只有通过认证的用户才有权进行相应操作，通常适用于企业间的合作网络，其安全性和私密性比公有链高。联盟链的去中心化程度在公有链和私有链之间，由若干机构或组织构成，数据只允许认证通过的联盟机构操作，交易速度快，而且由于节点的加入需要一定权限，因此联盟链中各节点的信任度高，容易达成共识，但是规模大小有限。

虽然单链模式在区块链中有着不错的安全性、数据防篡改能力和各自的特色，但是各单链模式仍存在不足。本文基于联盟链和云制造服务平台的需求，设计了用户数据链和交易数据链的双链模式，融合了联盟链的优点，并对其进行进一步地优化，将云制造平台中不同隐私程度的数据分开存放，既可以保持公开数据的透明性，又可以实现隐私数据的保密性，增加了云制造服务平台的安全性。

公有链、私有链、联盟链和本文所设计的双链模式的比较见表 1。

5.4　QoS 指标评估方法测试

在实际应用中，服务交易在第一次产生时，由于没有历史记录可以计算 QoS 值，所以往往需要由服务提供者自己设定一个初始的 QoS 值，也就是静态的 QoS 值。但是，初始的 QoS 值往往具有一定的主观性，随着服务调动次数的增加，应当适当减少初始 QoS 值的权重，以免由于初始 QoS 值的设定不合理或者过于主观，使 QoS 综合数值的真实性有所下降，从而对用户的判断产生影响。本节假设服务提供者在冷启动阶段设置的 QoS 值过高，测试冷启动问题对 QoS 综合数值的影响，其实验结果如图 6 所示，分为以下两种情况。

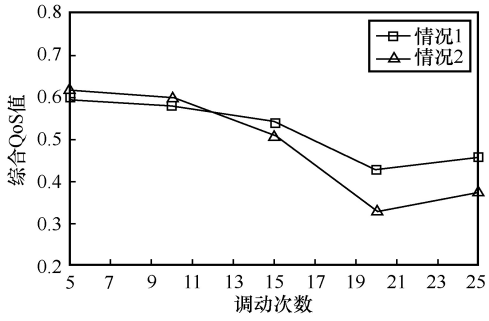


图 6　冷启动问题对 QoS 综合数值的影响

表 1　　**公有链、私有链、联盟链和本文所设计的双链模式的比较**

区块链模式	特点	不足	适用场景
公有链	完全去中心化，不受监管，公开透明，信息难以篡改	交易速度慢，安全性低	可信度要求高，但其交易无须很高的实时性的场景，如比特币和以太坊
私有链	私密性较高，交易速度快，具有权限管理，数据可修改，成本较低	具有局限性，公开透明性较低，规模大小受限	需要设置权限的场景，如金融、审计机构
联盟链	私密性较高，交易速度快，具有权限管理，可控性强，部分去中心化	规模大小受限，可能遭受合谋攻击，灵活性低	行业内不同企业间的交易和管理
双链	数据同步时间和处理速度较快，节省存储空间，根据数据隐私级别分类存放，安全性较高	数据存储结构较单链模式更复杂	需要对交易分类，数据部分公开，保护隐私数据，对读写速度和安全性要求较高的场景，如云制造服务

情况 1：不根据服务的调动次数减少静态 QoS 的权重。

情况 2：根据服务的调动次数减少静态 QoS 的权重，按照式(6)计算。

根据图 6 可以看出，在未对静态 QoS 的比重做出调整时（即情况 1），由于服务提供者将初始 QoS 值设定较高以提升自己的竞争力，因此前期综合 QoS 值较高。然而，通过设定静态 QoS 的比重随服务调动次数的增加而减少（即情况 2），更看重真实的历史交易情况后，后期其综合 QoS 值明显比情况 1 低，这反映出情况 1 的 QoS 值的真实性和参考价值不足。

综上所述，情况 2 中所设计的综合 QoS 计算方法有更高的可信度和合理度，计算结果更接近服务提供者实际的服务水平，可以解决冷启动问题对 QoS 综合数值造成的影响，为 PBFT 共识节点筛选和服务需求者寻求制造服务资源提供了可靠的判断依据，同时也增加了共识集群的可靠性。

5.5　共识时延与吞吐量测试

1) 共识时延测试

共识时延是指主节点开始进行共识操作到共识结束花费的所有时间，这个时间越低，区块链将数据上链的速度就越快，运行效率也越高。本节针对传统 PBFT 共识算法、文献[44]、文献[45]和本文所提的改进后的 PBFT 共识算法进行对比。区块链中的总节点数从 0 增加到 40，共识集群 C 的大小为 20（即综合信誉值大于 γ 的节点有 20 个），共识时延对比如图 7 所示。

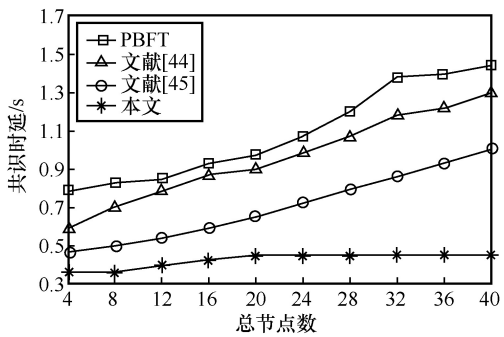


图 7　共识时延对比

显而易见，本文所改进的 PBFT 共识算法的共识时延比其他 3 种 PBFT 共识算法更低。当区块链中的节点数小于 20 时，4 种 PBFT 共识算法的共识时延都呈上涨趋势；当节点数大于 20 时，由于本文所设计的 PBFT 共识算法的共识集群数设为了 20，所以即使节点数不断增加，共识集群的数量也已经固定，从而共识时延会稳定在 0.45 s 左右。

2) 吞吐量测试

吞吐量是用于评价云制造服务平台交易处理能力的重要指标，其吞吐量越大，平台的交易处理能力就越高。本节设定总节点数 n=100，其中有 30 个节点的带宽为 0 MB，以模拟高错误率的情况，测试本文与传统 PBFT 共识算法、文献[44]、文献[45]在 30 min 内的吞吐量变化情况，对比如图 8 所示。

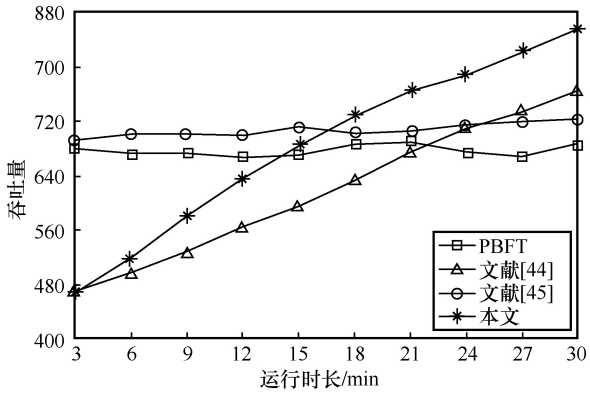


图 8　吞吐量对比

由于本测试是在高错误率的前提下进行的，因此在前期时恶意节点较多，文献[44]根据节点的信誉值决定话语权和主节点，本文根据综合信誉值选取主节点，当系统运行时间了一段时间后，节点产生了更多的共识行为记录，由此可以根据历史情况逐渐剔除掉综合信誉值低的节点，所以文献[44]与本文的吞吐量随着时间的增加而增加。同时，因为本文缩小了共识节点规模并简化了一致性协议流程，所以本文所改进的 PBFT 共识算法的吞吐量比文献[44]的吞吐量要高。另外，文献[45]产生主节点的方式与传统 PBFT 共识算法相似，但基于某些特性进行了聚类，并且优化了一致性协议流程，所以吞吐量受时间的影响不大，且其值略高于传统 PBFT 共识算法。

6　结束语

随着区块链技术和云制造服务新模式的发展，如何利用区块链技术增强云制造服务平台的安全性、可靠性、可用性和稳健性，成为许多学者研究的方向。针对当前云制造交易中存在的信任危机和数据处理问题，本文将区块链技术引入云制造服务

平台，对基于区块链技术的云制造服务架构及共识算法展开研究，主要内容包括基于双链模式的云制造服务平台架构设计、综合信誉值的计算、对传统 PBFT 共识算法的改进与具体的制造资源寻租和匹配步骤。分析和实验表明，该研究有效提高了云制造服务平台的运行效率和数据同步速度，节省了数据存储空间，增加了各企业间的信任度，为平台中的交易提供了更加安全的环境。接下来，将研究如何以更低的成本将智能合约部署到云制造服务平台，进一步完善平台的服务组合功能，并设置相应的奖惩机制，以此激发各服务提供者提高自身能力，保持良好的交易和共识行为。

参考文献：

[1] 李伯虎, 张霖, 王时龙, 等. 云制造: 面向服务的网络化制造新模式[J]. 计算机集成制造系统, 2010, 16(1): 1-7, 16.
LI B H, ZHANG L, WANG S L, et al. Cloud manufacturing: a new service-oriented networked manufacturing model[J]. Computer Integrated Manufacturing Systems, 2010, 16(1): 1-7, 16.

[2] ZHANG L, LUO Y L, TAO F, et al. Cloud manufacturing: a new manufacturing paradigm[J]. Enterprise Information Systems, 2014, 8(2): 167-187.

[3] 智研观点. 2021 年中国云制造行业发展现状及云制造企业对比分析（能科股份 VS 海得控制）[EB]. 2021 .
Intelligent Research View. Development status of China's cloud manufacturing industry in 2021 and comparative analysis of cloud manufacturing enterprises (Nancal Technology Co.,Ltd VS Hi-tech Control System Co., Ltd)[EB]. 2021.

[4] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[J]. Decentralized Business Review, 2008: 21260.

[5] 蔡晓晴, 邓尧, 张亮, 等. 区块链原理及其核心技术[J]. 计算机学报, 2021, 44(1): 84-131.
CAI X Q, DENG Y, ZHANG L, et al. Blockchain principle and core technology[J]. Chinese Journal of Computers, 2021, 44(1): 84-131.

[6] YAGA D, MELL P, ROBY N, et al. Blockchain technology overview[R]. National Institute of Standards and Technology, 2018.

[7] 蔡婷, 林晖, 陈武辉, 等. 区块链赋能的高效物联网数据激励共享方案[J]. 软件学报, 2021, 32(4): 953-972.
CAI T, LIN H, CHEN W H, et al. Efficient blockchain-empowered data sharing incentive scheme for Internet of Things[J]. Journal of Software, 2021, 32(4): 953-972.

[8] DAI H N, ZHENG Z B, ZHANG Y. Blockchain for internet of things: a survey[J]. IEEE Internet of Things Journal, 2019, 6(5): 8076-8094.

[9] TAN L, SHI N, YU K P, et al. A blockchain-empowered access control framework for smart devices in green internet of things[J]. ACM Transactions on Internet Technology, 2021, 21(3): 1-20.

[10] 杨小东, 席婉婷, 王嘉琪, 等. 基于签密和区块链的车联网电子证据共享方案[J]. 通信学报, 2021, 42(12): 236-246.
YANG X D, XI W T, WANG J Q, et al. Electronic evidence sharing scheme of internet of vehicles based on signcryption and blockchain[J]. Journal on Communications, 2021, 42(12): 236-246.

[11] SONG Y N, ZHANG F R, LIU C C. The risk of block chain financial market based on particle swarm optimization[J]. Journal of Computational and Applied Mathematics, 2020, 370: 112667.

[12] 沈蒙, 桑安琪, 祝烈煌, 等. 基于动机分析的区块链数字货币异常交易行为识别方法[J]. 计算机学报, 2021, 44(1): 193-208.
SHEN M, SANG A Q, ZHU L H, et al. Abnormal transaction behavior recognition based on motivation analysis in blockchain digital currency[J]. Chinese Journal of Computers, 2021, 44(1): 193-208.

[13] XIE M H, LI H Y, ZHAO Y J. Blockchain financial investment based on deep learning network algorithm[J]. Journal of Computational and Applied Mathematics, 2020, 372: 112723.

[14] 张健毅, 王志强, 徐治理, 等. 基于区块链的可监管数字货币模型[J]. 计算机研究与发展, 2018, 55(10): 2219-2232.
ZHANG J Y, WANG Z Q, XU Z L, et al. A regulatable digital currency model based on blockchain[J]. Journal of Computer Research and Development, 2018, 55(10): 2219-2232.

[15] ZHANG Q, LIAO B Y, YANG S L. Application of blockchain in the field of intelligent manufacturing: theoretical basis, realistic plights, and development suggestions[J]. Frontiers of Engineering Management, 2020, 7(4): 578-591.

[16] VATANKHAH B R. A blockchain technology based trust system for cloud manufacturing[J]. Journal of Intelligent Manufacturing, 2022, 33(5): 1451-1465.

[17] 刘敖迪, 杜学绘, 王娜, 等. 基于区块链的大数据访问控制机制[J]. 软件学报, 2019, 30(9): 2636-2654.
LIU A D, DU X H, WANG N, et al. Blockchain-based access control mechanism for big data[J]. Journal of Software, 2019, 30(9): 2636-2654.

[18] KARAFILOSKI E, MISHEV A. Blockchain solutions for big data challenges: a literature review[C]//Proceedings of IEEE EUROCON 2017-17th International Conference on Smart Technologies. Piscataway: IEEE Press, 2017: 763-768.

[19] JING N, LIU Q, SUGUMARAN V. A blockchain-based code copyright management system[J]. Information Processing & Management, 2021, 58(3): 102518.

[20] KAMATH R. Food traceability on blockchain: walmart's pork and mango pilots with IBM[J]. The Journal of the British Blockchain Association, 2018, 1(1): 1-12.

[21] LIU X L, BARENJI A V, LI Z, et al. Blockchain-based smart tracking and tracing platform for drug supply chain[J]. Computers & Industrial Engineering, 2021, 161: 107669.

[22] 陈友荣, 陈浩, 韩蒙, 等. 基于信用等级划分的医疗数据安全共识

算法[J]. 电子与信息学报, 2022, 44(1): 279-287.
CHEN Y R, CHEN H, HAN M, et al. Security consensus algorithm of medical data based on credit rating[J]. Journal of Electronics & Information Technology, 2022, 44(1): 279-287.

[23] LIN P, SONG Q Y, YU F R, et al. Task offloading for wireless VR-enabled medical treatment with blockchain security using collective reinforcement learning[J]. IEEE Internet of Things Journal, 2021, 8(21): 15749-15761.

[24] 张超, 李强, 陈子豪, 等. Medical Chain: 联盟式医疗区块链系统[J]. 自动化学报, 2019, 45(8): 1495-1510.
ZHANG C, LI Q, CHEN Z H, et al. Medical chain: alliance medical blockchain system[J]. Acta Automatica Sinica, 2019, 45(8): 1495-1510.

[25] 魏欣, 王心妍, 于卓, 等. 基于联盟链的物联网跨域认证[J]. 软件学报, 2021, 32(8): 2613-2628.
WEI X, WANG X Y, YU Z, et al. Cross domain authentication for IoT based on consortium blockchain[J]. Journal of Software, 2021, 32(8): 2613-2628.

[26] CASTRO M, LISKOV B. Practical Byzantine fault tolerance and proactive recovery[J]. ACM Transactions on Computer Systems, 2002, 20(4): 398-461.

[27] TAO F, ZHANG L, VENKATESH V C, et al. Cloud manufacturing: a computing and service-oriented manufacturing model[J]. Proceedings of the Institution of Mechanical Engineers, Part B: Journal of Engineering Manufacture, 2011, 225(10): 1969-1976.

[28] TAO F, LAILI Y J, XU L D, et al. FC-PACO-RM: a parallel method for service composition optimal-selection in cloud manufacturing system[J]. IEEE Transactions on Industrial Informatics, 2013, 9(4): 2023-2033.

[29] ZHANG G, ZHANG Y F, XU X, et al. An augmented Lagrangian coordination method for optimal allocation of cloud manufacturing services[J]. Journal of Manufacturing Systems, 2018, 48: 122-133.

[30] LIU Y K, WANG L H, WANG X V, et al. Scheduling in cloud manufacturing: state-of-the-art and research challenges[J]. International Journal of Production Research, 2019, 57(15/16): 4854-4879.

[31] MOURAD M H, NASSEHI A, SCHAEFER D, et al. Assessment of interoperability in cloud manufacturing[J]. Robotics and Computer-Integrated Manufacturing, 2020, 61: 101832.

[32] DELARAM J, HOUSHAMAND M, ASHTIANI F, et al. A utility-based matching mechanism for stable and optimal resource allocation in cloud manufacturing platforms using deferred acceptance algorithm[J]. Journal of Manufacturing Systems, 2021, 60: 569-584.

[33] BAI J, FANG S L, XU X, et al. LMPF: a novel method for bill of standard manufacturing services construction in cloud manufacturing[J]. Journal of Manufacturing Systems, 2022, 62: 402-416.

[34] HARDJONO T, SMITH N. Cloud-based commissioning of constrained devices using permissioned blockchains[C]//IoTPTS '16: Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security. 2016: 29-36.

[35] LI Z, BARENJI A V, HUANG G Q. Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform[J]. Robotics and Computer-Integrated Manufacturing, 2018, 54: 133-144.

[36] YU C X, ZHANG L P, ZHAO W F, et al. A blockchain-based service composition architecture in cloud manufacturing[J]. International Journal of Computer Integrated Manufacturing, 2020, 33(7): 701-715.

[37] TAN W A, ZHU H, TAN J J, et al. A novel service level agreement model using blockchain and smart contract for cloud manufacturing in industry 4.0[J]. Enterprise Information Systems, 2022, 16(12): 1939426.

[38] RADMANESH S A, HAJI A, FATAHI VALILAI O. Blockchain-based cloud manufacturing platforms: a novel idea for service composition in XaaS paradigm[J]. PeerJ Computer Science, 2021, 7: e743.

[39] 何泾沙, 张琨, 薛瑞昕, 等. 基于贡献值和难度值的高可靠性区块链共识机制[J]. 计算机学报, 2021, 44(1): 162-176.
HE J S, ZHANG K, XUE R X, et al. A highly reliable consensus mechanism for blockchain based on contribution and difficulty values[J]. Chinese Journal of Computers, 2021, 44(1): 162-176.

[40] KING S, NADAL S. Ppcoin: peer-to-peer crypto-currency with proof-of-stake[EB]. 2012.

[41] Fabric official website[EB]. 2022.

[42] 闵新平, 李庆忠, 孔兰菊, 等. 许可链多中心动态共识机制[J]. 计算机学报, 2018, 41(5): 1005-1020.
MIN X P, LI Q Z, KONG L J, et al. Permissioned blockchain dynamic consensus mechanism based multi-centers[J]. Chinese Journal of Computers, 2018, 41(5): 1005-1020.

[43] LI W Y, FENG C L, ZHANG L, et al. A scalable multi-layer PBFT consensus for blockchain[J]. IEEE Transactions on Parallel and Distributed Systems, 2021, 32(5): 1146-1160.

[44] 赖英旭, 薄尊旭, 刘静. 基于改进 PBFT 算法防御区块链中 sybil 攻击的研究[J]. 通信学报, 2020, 41(9): 104-117.
LAI Y X, BO Z X, LIU J. Research on sybil attack in defense blockchain based on improved PBFT algorithm[J]. Journal on Communications, 2020, 41(9): 104-117.

[45] 张磊, 郑志勇, 袁勇. 基于区块链的电子医疗病历可控共享模型[J]. 自动化学报, 2021, 47(9): 2143-2153.
ZHANG L, ZHENG Z Y, YUAN Y. A controllable sharing model for electronic health records based on blockchain[J]. Acta Automatica Sinica, 2021, 47(9): 2143-2153.

[46] SUKHWANI H, MARTÍNEZ J M, CHANG X L, et al. Performance modeling of PBFT consensus process for permissioned blockchain network (hyperledger fabric)[C]//Proceedings of 2017 IEEE 36th Symposium on Reliable Distributed Systems. Piscataway: IEEE Press, 2017: 253-255.

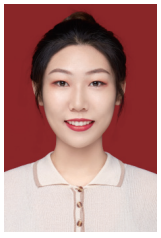
[47] KAMVAR S D, SCHLOSSER M T, GARCIA-MOLINA H. The Eigentrust algorithm for reputation management in P2P net-

works[C]//WWW '03: Proceedings of the 12th international conference on World Wide Web. 2003: 640-651.

[48] LIU Y T, NGU A H, ZENG L Z. QoS computation and policing in dynamic web service selection[C]//WWW Alt. '04: Proceedings of the 13th international World Wide Web conference on Alternate track papers & posters. 2004: 66-73.

作者简介：

蒋伟进（1964– ），男，博士，湖南工商大学二级教授，主要研究方向为区块链技术、云计算、边缘计算、群体智能感知、社会计算、网络安全。



周文颖（1999– ），女，湖南工商大学硕士生，主要研究方向为区块链技术、云制造。

李恩（1995– ），男，湖南工商大学硕士生，主要研究方向为区块链技术、物联网。

罗田甜（1998– ），女，湖南工商大学硕士生，主要研究方向为区块链技术、物联网。

杨莹（1999– ），女，湖南工商大学硕士生，主要研究方向为复杂网络、区块链技术。