计算机科学
COMPUTER SCIENCE

面向食品溯源场景的 PBFT 优化算法应用研究

李博，向海昀，张宇翔，廖浩德

引用本文

李博，向海昀，张宇翔，廖浩德. 面向食品溯源场景的 PBFT 优化算法应用研究[J]. 计算机科学, 2022, 49(6A): 723-728.

LI Bo, XIANG Hai-yun, ZHANG Yu-xiang, LIAO Hao-de. Application Research of PBFT Optimization Algorithm for Food Traceability Scenarios[J]. Computer Science, 2022, 49(6A): 723-728.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.210800018

面向食品溯源场景的 PBFT 优化算法应用研究

李 博 向海昀 张宇翔 廖浩德
西南石油大学计算机科学学院 成都 610500
(310558973@qq.com)

摘 要 区块链不可篡改、可追溯等特性能较好地支撑食品溯源系统,在食品溯源与区块链技术相结合的应用中存在着延时长、节点多、系统开销大等问题。针对上述问题,基于实用拜占庭容错算法(Practical Byzantine Fault Tolerance,PBFT),提出一种适用于食品溯源场景的优化 PBFT 算法 trace-PBFT(t-PBFT)。首先,将供应链中节点划分为 3 个等级,根据节点在共识中的实际通信量动态更新节点状态,并以此来评价节点的可靠性,作为选举主节点的依据;其次,结合食品供应链的特点,优化原算法中的一致性协议,减少节点通信次数。实验结果表明,相比 PBFT 算法,t-PBFT 算法在通信开销、请求延时、吞吐量等方面表现更优;最后,基于 t-PBFT 算法且结合联盟链提出一种满足食品溯源需求的架构模型,对食品供应链中各环节进行数据记录,保证数据可追溯,确保食品流通过程的安全性。

关键词:区块链应用;食品溯源;共识算法;实用拜占庭容错;联盟链
中图法分类号 TP312

Application Research of PBFT Optimization Algorithm for Food Traceability Scenarios

LI Bo,XIANG Hai-yun,ZHANG Yu-xiang and LIAO Hao-de
School of Computer Science,Southwest Petroleum University,Chengdu 610500,China

Abstract The characteristics of blockchain such as immutability and traceability can better support the food traceability system, and there are problems such as long delay,many nodes and high system overhead in the application of food traceability combined with blockchain technology. To address the above problems,an optimized PBFT algorithm trace-PBFT(t-PBFT) is proposed for the food traceability scenario based on the practical Byzantine fault tolerance(PBFT) algorithm. Firstly,the nodes in the supply chain are divided into three classes,and the node status is dynamically updated according to the actual communication volume of the nodes in the consensus,which is used to evaluate the reliability of the nodes as the basis for electing the master node. Secondly,the consistency protocol in the original algorithm is optimized to reduce the number of node communications by combining the characteristics of the food supply chain. Experimental results show that the t-PBFT algorithm performs better than the PBFT algorithm in terms of communication overhead,request delay and throughput. Finally,based on the t-PBFT algorithm and combined with the consortium chain,an architectural model to meet the demand of food traceability is proposed. It can record the data of each link in the food supply chain,ensure data traceability and the safety of food circulation process.

Keywords Blockchain application,Food traceability,Consensus algorithm,Practical Byzantine fault tolerance,Consortium chain

自 2008 年中本聪发表比特币白皮书以来[1],作为分布式系统典范的比特币系统在全球发展迅速且运行稳定,而其底层技术更加受到业界的关注。区块链技术的诞生是为了应对现有中心化体系所带来的资源垄断等问题[2]。它是 P2P 网络、共识机制、加密算法、智能合约等多种技术的组合,具有去中心化、不可篡改、可追溯等特点。简而言之,其本质是一种以链式结构为基础的分布式账本[3]。针对区块链技术的使用场景不同,其可分为公有链、联盟链和私有链[4]。公有链系统是完全开放去中心的系统,任何节点都访问数据且可参与系统的维护,但其效率较低。联盟链和私有链都需要相关授权才能进入网络,两者的节点数量比对公有链更加固定,审查更为严格[5]。不同的是,联盟链一般应用于企业或组织之间,而私有链只应用于企业或组织内部。供应链上企业数量多,信息交互频繁,选择联盟链系统更加符合供应链的业务场景。针对原有中心化供应链平台上下游信息分散、共享程度不高、真实性、可靠性差等问题[6],Liao[7] 提出基于区块链技术的商品可信溯源方案,建立商品溯源平台,将商品供应链各环节数据分别采集并存储于区块链中,实现信息可查询、不可篡改,保证数据真实可信。Li 等[8] 提出基于区块链的汽车供应链产品追溯系统,采用区块链+汽车供应链的模式,对汽车相关数据进行分布式存储,保证了供应链数据的安全性,增加参与方的互相信任,使得汽车产品的溯源更加高效便捷。Yu 等[9] 提出基于区块链的医药溯源系统,以联盟链平台为基础,对药品供应链上的各个环节进行数据记录追踪,保证药品安全。

基金项目:教育部产学合作协同育人项目(201801209004)
This work was supported by the Ministry of Education Industry-University Cooperation Collaborative Education Project(201801209004).
通信作者:向海昀(652674247@qq.com)

Wang 等[10]提出农产品柔性可信溯源方案，结合区块链技术的优良特性，适用于农产品追溯中的相关业务需求。

以上文献都将区块链技术与供应链场景进行不同程度的结合，对现有溯源系统进行了改进，而相对忽视了共识算法对整个分布式系统的影响。共识算法作为区块链系统的核心组件[11]，其作用是保证系统中所有节点能够达成状态一致。现区块链中主要共识算法包括 PoW，PoS[12]，Raft[13] 和 PBFT[14]算法等，这些算法将直接影响整个系统的可靠性和可用性。实用拜占庭容错(PBFT)共识算法是由 BFT 算法改进而来[15]，现作为联盟链中较为主流的共识算法，被广泛应用，能够较大程度上解决拜占庭将军问题[16]，但存在通信开销大、效率低等缺陷[17]。针对 PBFT 算法中存在的问题，并结合食品供应链中节点相对可信的特点，提出一种改进的 PBFT 算法，以减少原有 PBFT 算法的通信开销，提升节点共识效率，更好地满足行业需求。

1 PBFT 算法

实用拜占庭容错算法(PBFT)是由 Castro 和 Liskov 于 1999 年提出的，其目的是解决分布式系统中存在的拜占庭将军问题，是目前解决拜占庭问题的经典算法。拜占庭将军问题证明存在 f 个拜占庭节点时，网络中需要的节点总数 $N \geqslant 3f+1$，才可保证系统正常可用，则能容忍的最大拜占庭节点数量为 $(N-1)/3$。

PBFT 是一种基于状态机副本复制的分布式算法，即每个状态机副本保存服务状态，从而实现用户的合法请求。各节点达成共识过程中，PBFT 将运行 3 种协议，分别为一致性协议、检查点协议和视图切换协议。

1.1 一致性协议

在此算法中存在主节点和从节点两种角色，当客户端向主节点发起请求后，将会执行一致性协议，完整的协议执行过程分为客户端请求、预准备、准备、提交、回复 5 个阶段，执行过程如图 1 所示。

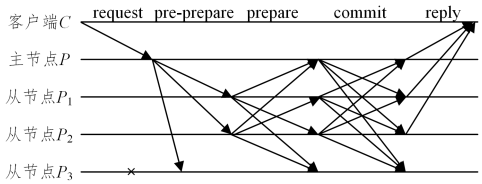

图 1 PBFT 算法一致性协议执行过程

Fig. 1 Execution process of the consensus protocol of PBFT algorithm

(1)客户端请求阶段：客户端向主节点发送服务请求 $\langle REQUEST, o, t, c \rangle$，$o$ 为请求的具体操作，t 为时间戳，c 为客户端标识。

(2)预准备阶段：主节点为从客户端收到的请求分配提案编号，然后发出预准备消息 $\langle\langle PRE\text{-}PREPARE, v, n, d\rangle, m\rangle$ 给各副本节点，其中 v 为视图编号，n 为消息编号，d 为消息的摘要，m 为客户端的请求消息。

(3)准备阶段：从节点收到预准备消息后，则向其他节点发送准备消息 $\langle PREPARE, v, n, d, i\rangle$，同时接收来自其他节点的准备信息。收到准备消息的节点会将收到的消息与预准备消息进行对比。验证通过后，则把这条准备消息写入消息日志中。当收到至少 $2f+1$ 条准备消息后，则进入确认阶段。

(4)提交阶段：此阶段中节点向包括主节点在内的其他节点发送消息 $\langle COMMIT, v, n, d, i\rangle$，若节点收到了包括自身在内的 $2f+1$ 条 *COMMIT* 消息后，则请求在此节点上达到 committed 状态，进入下一阶段。

(5)回复阶段：完成确认后，各节点向客户端发送消息 $\langle REPLY, v, t, c, i, r\rangle$，其中 r 为客户端请求的执行结果。

1.2 视图切换协议

在 PBFT 共识过程中，所有节点的状态必须保持一致，即处于同一个视图(View)中。当从节点 i 在视图 v_{old} 中超时未收到主节点发送的请求，则从节点将进行视图更换协议，视图编号 $v+1$，并开始选举新的主节点。设所有节点集合为 N，节点编号为 $\{0,1,2,\cdots,|N|-1\}$，$v_{new}=v_{old}+1$，新的主节点编号的计算式为：

$$p = v_{new} \bmod |N| \tag{1}$$

其中，p 为主节点编号，v_{new} 为更新的视图，$|N|$ 为节点总数。

1.3 检查点协议

系统中的节点在共识中产生的共识信息保存在从节点的日志中，会占用节点的存储空间。系统长期运行则会产生大量的日志信息。检查点协议周期性地工作，能够帮助节点清除无用日志，释放节点内存资源，并且帮助某些自身存在故障或因网络问题而未和系统同步的节点。节点在执行视图转换协议中，检查点协议能保证节点执行视图切换前的相关请求，保其请求顺序与之前一致。

2 改进的 PBFT 算法

PBFT 算法被广泛应用于联盟链中，其容错性能够降低拜占庭节点对网络的影响，确保系统的可信性。但在共识过程中，首先需要选举主节点，选举主节点是基于节点编号，选举恶意节点的概率偏高，会影响系统可靠性；其次，当有客户端请求时，节点需要进行多个阶段通信，通信次数较高，尤其当网络中节点数增加时，共识效率会进一步降低；最后，网络中视图的频繁切换会导致通信开销增大，服务响应变慢。

2.1 算法概述

在食品溯源场景下，系统中各企业受到相关部门审查或监管，主动作恶节点会受到相应的惩罚，从而可以较大程度地排除主动作恶的节点。但不可否认的是，当节点存在自身故障或网络延时，同样存在导致客户端服务请求失败的情况。鉴于这两方面的实际情况，提出溯源实用拜占庭算法(Trace-practical Byzantine Fault Tolerance，t-PBFT)。

(1)考虑到节点自身故障与网络延时始终存在，设置节点评级机制，用于评价节点是否处于故障状态。改进主节点的选举方式，避免选举存在故障的主节点，降低视图切换的频率，从而降低故障主节点对系统响应的影响。

(2)在原 PBFT 算法中前两阶段已经完成了节点间的消息广播及交互，第三阶段与视图切换协议共同保证不同视图下请求的执行安全。视图正常变更不会出现安全问题，仅在主节点崩溃时才会出现安全问题。若主节点崩溃执行视图切换协议时，某从节点会向各节点广播视图切换消息，该消息包含该从节点所得到的最后一个请求序号，主节点被选举时将明确该序号已被使用。而食品供应链场景下各成员节点进行

身份认证并受到监管，节点可信度相对较高，不存在主动作恶，被选举的主节点在进行下次共识时不会再次使用该请求序号，从而保证不同视图下请求的正确执行。由此可考虑将原有 PBFT 算法的第三通信阶段进行合并，削减一致性协议过程中的通信开销，达到提升系统吞吐量、降低延时的目的。

2.2　节点评价机制

对于食品供应链节点中可能出现的故障问题，引入评价机制来描述节点的状态，为节点分配其对应行为的积分，对节点的行为进行奖励或惩罚，并根据节点的积分高低来择优选举主节点，由此来增强节点行为的积极性，并降低选举故障主节点的概率。

2.2.1　初始积分设置

t-PBFT 算法主要应用于食品供应链中各级厂商的联盟链环境中，而不同食品厂商的综合实力及社会信誉存在一定的差异。通常来说，某厂商节点的综合实力越强，其具有的性能和稳定性则越强。鉴于此实际情况，将食品供应链中企业的综合实力及社会信誉作为初始积分的评价指标。

S_i 表示编号为 i 节点的积分值，n 表示网络中节点个数。网络初始化评分时，将所有企业按照综合实力进行排序，取前 $\frac{1}{3}n$ 节点作为优秀节点，并随机设置初始积分大于 80 且小于 100，积分精度精确到 0.1，剩余节点初始积分按序设置为小于等于 80 且大于 0，积分递减步长为 0.1。若 $80<S_i\leqslant 100$，则表示该节点状态优秀，能够优先被选举为主节点；若 $0<S_i\leqslant 80$，节点作为普通节点参与共识；若 $S_i=0$，表示该节点在共识过程中发生过多次故障，此时该节点将被标记为无效节点，不再参与共识过程，若需要重新进入网络中，则需要供应链中节点对其投票进行重新认证。节点行为状态转换如图 2 所示。

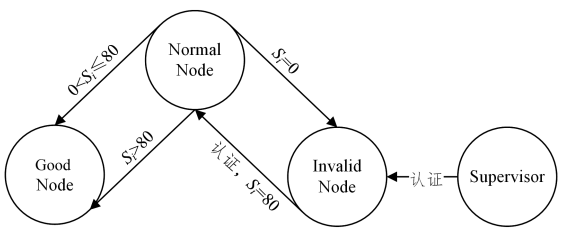

图 2　节点行为状态转换

Fig. 2　Diagram of node behavior state transition

2.2.2　积分更新规则

每次共识完成后，通过检查点协议对节点积分进行更新。若节点进行了共识行为，则对节点奖励加分，否则对节点减分。可通过检查节点日志信息，计算共识过程中的节点通信次数与预期通信次数是否相同，来判断其行为状态。为防止节点恶意广播积分值，会生成积分值有序列表存于各节点，进行消息广播时需要包含积分值。

(1)积分增加：通过判断节点的实际通信次数，来判断该节点共识过程中的行为，t-PBFT 算法根据式(2)增加节点积分。

$$S_i'=\begin{cases}S_i+\dfrac{An}{Hn}\times X_1, & S_i<80\\ S_i+\dfrac{An}{Hn}\times X_2, & 80\leqslant S_i<100\end{cases}\tag{2}$$

其中，S_i' 为节点 i 更新后的积分值，S_i 为更新前的积分值，An 为节点共识过程中的实际通信次数，Hn 为节点共识过程中的期望通信次数。若节点进行一次完整的共识过程，两者比值为 1，X 为固定常数，用于调整节点积分的增长幅度，通常由供应链中的成员协商决定。通过设置 $X_1>X_2$，鼓励普通节点进行正确共识可以获得比优秀节点更多的积分。

(2)积分降低：当节点的实际通信次数 $An=0$ 时，则说明该节点在共识过程中存在故障，则依据式(3)对节点积分进行扣除。

$$S_i'=\begin{cases}S_i-Y_1, & S_i<80\\ S_i-Y_2, & 80\leqslant S_i<100\end{cases}\tag{3}$$

其中，Y 为固定常数，同时设置 $Y_1<Y_2$，对优秀节点进行较多的惩罚。若主节点在共识过程中超时或出现故障，则主节点被扣除 40 分，变为普通节点。

2.3　主节点选举

在系统运行过程中，需尽可能减少主节点更换次数。在网络初始化或主节点发生故障时，则更换主节点(启动视图更换协议)。在 t-PBFT 算法中，每个节点会生成维护各个节点积分值的有序列表，并将此作为选举主节点的依据。积分值高表示该节点在近期共识过程中较为稳定，选举此类节点可极大地降低视图切换的概率，从而保证系统的稳定性，提升系统效率。

(1)网络初始化：在完成各节点积分的初始化之后，选择积分值最高的节点作为主节点，其余节点作为副本节点参与共识。

(2)主节点故障：此情况下副本节点发现主节点出现故障，向全网广播选举自身维护的有序列表中积分值最高的节点，此后流程与 PBFT 算法视图切换协议一致，故不再赘述。若系统经长时间运行迭代后，出现多个积分值最高且相等的节点，则从此部分中随机选择主节点。因出错后的惩罚分数较大，当执行视图更换协议时，能够保证已出错主节点在较长时间内无法竞选主节点。

2.4　共识协议优化

PBFT 算法为应对主动作恶节点而设计比较复杂的共识协议，其中提交阶段是让系统中各节点掌握其余节点的状态。而在食品溯源网络中，各成员受到监管，可信度高且运行环境较为稳定。同时，在引入节点评价机制后，降低了选举故障主节点的概率，因此在 t-PBFT 算法中考虑省略经典 PBFT 算法中的提交阶段，可较大程度地降低系统通信开销。优化的共识协议执行过程如图 3 所示。

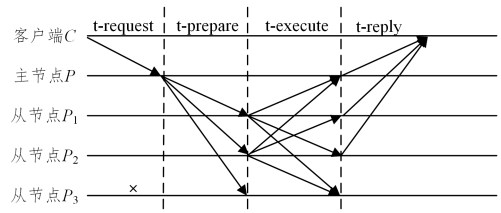

图 3　优化共识协议执行过程

Fig. 3　Optimized consensus protocol execution process

协议详细执行流程包括以下 4 个阶段。

(1)请求阶段(t-request)：客户端向主节点发送请求〈t-$REQUEST$，o，t，c〉。

(2)准备阶段(t-prepare)：主节点收到请求并对请求验证

后，将准备消息广播到网络中的所有节点，准备消息格式为〈〈*t-PREPARE*，v，n，$H(m)$，s〉，m〉，其中 $H(m)$ 为客户端请求消息的摘要，s 为节点积分值，从节点收到请求消息将信息存储到本地日志后进入执行阶段。

(3)执行阶段(t-execute)：此阶段中从节点收到准备消息后向包括主节点在内的所有节点发送执行消息，消息格式为〈*t-EXECUTE*，v，n，d，i，s〉，i 为节点编号，同时该节点也将接收其他节点所广播的执行消息。各节点需要对消息进行验证，直到节点收到 $2f+1$ 条通过验证的消息时，则认为共识达成，节点进入响应阶段。

(4)响应阶段(t-reply)：客户端接收来自各节点的响应结果〈*t-REPLY*，v，t，c，i，r〉，r 为节点响应结果。

2.5 算法流程

t-PBFT 算法基于溯源场景，在引入节点评价机制的同时，优化原有 PBFT 算法共识协议。通过对此两方面的改进，降低故障主节点的选举概率，并减少了相应的通信开销，进而达到提升系统效能的目的。t-PBFT 算法流程如图 4 所示。

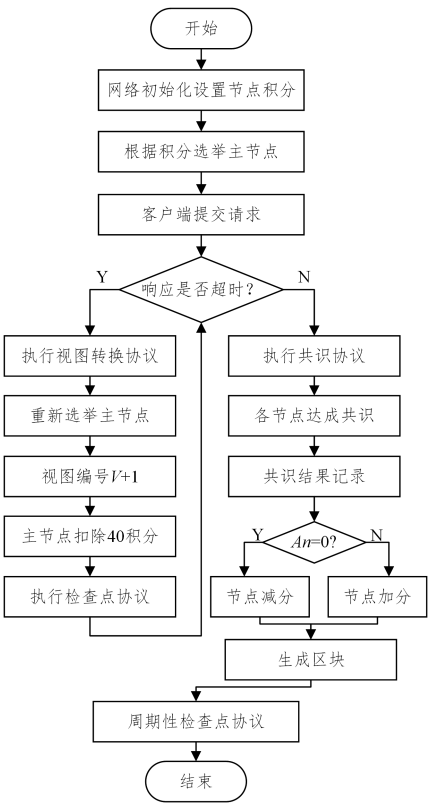

图 4 t-PBFT 算法流程

Fig. 4 Flow chart of t-PBFT algorithm

算法具体执行过程如下：

(1)对网络进行初始化设置，将节点的初始积分设置为 80，对网络中的 M 个节点用{0，1，2，…，$M-1$}进行编号，并按积分选择出主节点。

(2)客户端对主节点发起请求后，此时会判断主节点是否存在超时的情况：若存在超时，从节点发起视图转换协议消息重新选举主节点，消息中包含对主节点扣除 20 积分的请求，选举成功后视图编号 $v+1$，主节点扣除 20 积分，并执行检查点协议，恢复各节点在视图转换前的行为，请求继续。若主节点未超时，则请求正常进行。

(3)请求正常执行共识协议，共识协议执行成功后，各节点达成共识，对结果进行日志记录并返回结果给客户端。

(4)完成响应后，对各个节点在本次请求中的通信次数进行计算。若实际通信数 An 为 0，则对节点减分，若 $0<An\leqslant Hn$，则对节点加分。此过程完成对节点积分的更新。

(5)节点更新积分后，打包生成区块，并执行周期性检查点协议，其作用是进行垃圾回收，清除各节点在本次请求下的一些过时消息，释放节点空间，一次请求完成。

3 实验结果及分析

实验设备配置信息为 Intel Core i5-8400 处理器，8 GB 内存，Windows 10 操作系统，256 GB SSD 硬盘，用编程语言仿真模拟实现 t-PBFT 算法，并且通过 Docker 容器设置不同 IP 地址模拟区块链环境，确保 t-PBFT 算法和 PBFT 算法的实验环境相同。本文将从通信开销、请求延时、吞吐量 3 个方面对 PBFT 算法和 t-PBFT 算法进行实验，通过理论和实验结果分析两种算法的性能。

3.1 通信开销分析

通信开销指各节点在一次共识过程中所产生的通信次数总和，设网络中节点总数为 m，系统发生视图切换的概率为 p，由 1.1 节对经典 PBFT 算法的一致性协议介绍可知，request 阶段通信开销为 1，pre-prepare 阶段通信开销 $m-1$，prepare 阶段通信开销为 $m(m-1)$，commit 阶段与 prepare 阶段通信开销相同，均为 $m(m-1)$，reply 阶段通信开销为 m，而在发生视图切换时的通信开销为 $m(m-1)$，因此 PBFT 算法总的通信开销为：

$$C_p=(p+2)m^2-pm \tag{4}$$

t-PBFT 算法对一致性协议进行了简化，并引入了节点评价机制，由分析可知其能降低视图转换的概率。设其视图切换概率为 q，t-request 阶段通信开销为 1，t-prepare 阶段通信为 $m-1$，t-execute 阶段通信开销为 $m(m-1)$，t-reply 阶段通信开销为 m，切换视图通信开销为 $m(m-1)$，总的通信开销为：

$$C_{tP}=(q+1)m^2-(1-q)m \tag{5}$$

两种算法的通信开销比值 Q 如式(6)所示：

$$Q=\frac{C_{tP}}{C_p}=\frac{(q+1)m+1-q}{(p+2)m-p},0<q\leqslant p<1 \tag{6}$$

其中，p，q 分别为两种算法视图切换概率值，取值范围为 0～1，将 q 置换为 p，并对式(6)进行变换操作可得式(7)：

$$Q=1-\frac{m+1}{(p+2)m-p} \tag{7}$$

对式(7)做可视化分析得三维图，如图 5 所示。

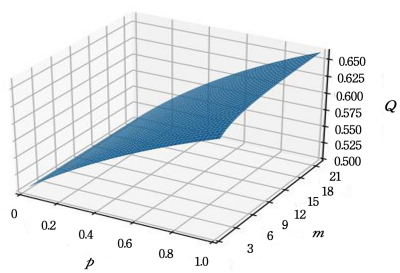

图 5 t-PBFT 与 PBFT 通信量比值三维图

Fig. 5 3D plot of t-PBFT and PBFT traffic ratio

由图 5 可知，节点数 m 取值有限，当视图切换概率 p 一

定时，随着节点数的增加，比值 Q 逐渐增大，但 Q 值始终小于 1。因此在多节点的食品供应链环境中，t-PBFT 算法通信次数始终少于 PBFT 算法。对式(7)求极限可得 $\lim\limits_{\substack{m\to\infty\\ p\to 1}} Q=\frac{2}{3}$，即 $Q_{\max}=\frac{2}{3}$，从理论上证明 t-PBFT 算法的通信开销比原算法减少了 33%，从而达到提升系统性能的目的。

3.2　请求延时

作为评价共识算法的关键参数之一，请求延时指客户端向主节点提交请求到系统完成共识返回结果的时间间隔。本次实验以节点数作为实验变量，测量算法在不同节点数下的请求延时。为减小实验误差，取 50 次请求的平均值作为请求时延的实验值，实验结果如图 6 所示。

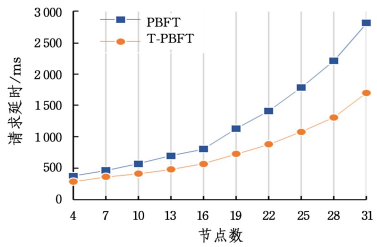

图 6　请求延时对比

Fig. 6　Diagram of request delay comparison

由实验结果分析可知，随着节点数的增加，请求延时逐渐增大。在节点数较少时，两种算法的请求延时相差较小，且该实验指标变化趋势较为平缓，但随着节点数量的逐渐增多，t-PBFT 算法请求延时的变化率小于 PBFT 算法，稳定性更佳，更适用于多节点环境。

3.3　吞吐量

吞吐量一般指单位时间内系统能处理完成请求的数量，用 TPS(Transaction Per Second)来表示。在算法的设计中，主节点引入视图的概念，使得系统能并发地处理客户端的请求，即吞吐量能够较好地描述系统这一特性。实验设置在不同节点数下，客户端发送 500 次请求，实验多次记录这些请求处理完成所需的时间并计算出平均吞吐量，实验结果如图 7 所示。

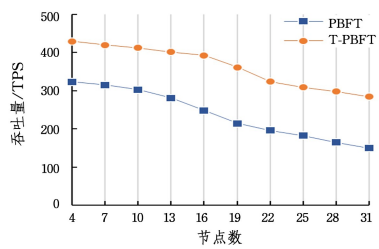

图 7　吞吐量对比

Fig. 7　Diagram of throughput comparison

由实验结果可知，在节点数较少时，两种算法的吞吐量都随着节点数的增多而呈现平缓下降的趋势，但在多节点环境下，PBFT 的吞吐量下降速率高于 t-PBFT 算法，平均吞吐量由 237 TPS 提升至 363 TPS。从总体来看，t-PBFT 算法比原算法更适用于食品溯源领域。

4　基于 t-PBFT 的食品溯源架构

对原有的 PBFT 算法进行优化后，针对食品溯源领域，本文提出一种基于 t-PBFT 算法的区块链技术食品溯源系统架构。

食品供应链上下游涉及多个企业，可简要划分为原料商、生产商、经销商、零售商、监管机构和消费者。使用区块链技术构建食品溯源系统，监管机构能实现对食品供应链的每个环节进行追溯，有效打破了信息孤岛的问题。若出现食品安全事故时，监管机构能够迅速定位责任企业，查明事故原因，从而降低事件影响。本文结合区块链技术的模型，选取联盟链作为系统基础设施，将区块链食品溯源系统架构分为 6 个部分进行设计，分别为数据采集层、数据层、网络层、合约层、应用层和用户层，具体的系统架构如图 8 所示。

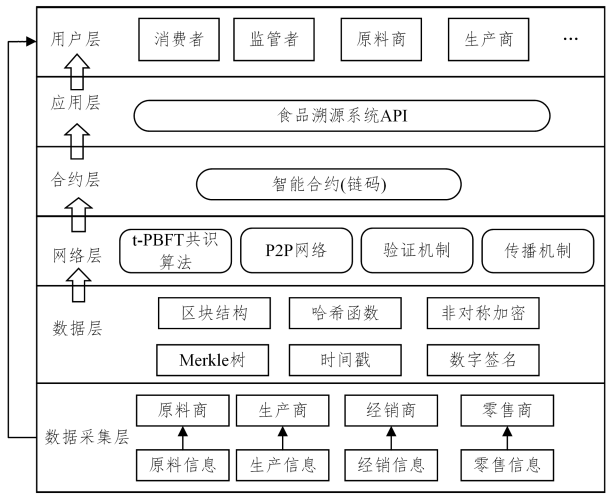

图 8　食品溯源系统架构

Fig. 8　Architecture of food traceability system

在此架构中，数据采集层指对食品供应链上的食品原料信息、生产信息、物流信息和销售信息进行采集，此阶段可使用相应的物联网技术进行信息收集。数据层指将下层采集的各环节食品信息存储在数据层，根据数据层的存储容量的大小判断是否使用传统数据库对详细信息进行存储，区块链系统上可只存储食品的关键信息或哈希摘要。网络层基于 P2P 网络，包含共识算法、验证机制和传播机制等，将 t-PBFT 算法插入此层中可减少节点共识通信开销，以达到提升溯源系统性能的目的。合约层指将食品供应链上的相关业务需求进行合约封装。智能合约是能够实现溯源系统的功能代码，在不需要第三方的情况下，达到某些约束条件自动执行相应的命令，可与下层结构进行交互。应用层提供了与区块链系统的交互接口，使得用户能够对区块链上的食品数据进行访问接入。用户层面向食品供应链中的各个角色，各企业可将采集的信息上传至系统中，其中消费者和监管机构可通过系统进行查询验证。

在图 8 所示的架构中，数据层及网络层是由系统中作为基础设施的联盟链提供，如目前主流的联盟链平台 Hyperledger Fabric，其组件具有可拔插的特性，其中包括共识算法，用户可按照相关的业务需求对各组件进行定制改进。而本文结合其他食品溯源方案提出该架构，并在网络层中嵌入 t-PBFT 算法，相较于以往的区块链食品溯源系统而言，改进的共识算法的优势在于可改善食品溯源供应链中通信开销大而导致的性能低下、系统消耗高问题，从而提升食品供应链联

盟中各节点的共识效率，能够更好地满足行业的相关需求。此外，数据采集层、合约层和应用层可分别由物联网技术、合约编码及软件开发员等负责，架构中各个部分共同保证数据的真实性、可追溯性和不可篡改性。

结束语 本文在 PBFT 算法的基础上，结合有监管下的食品供应链中节点相对可信的特点，提出一种适用于食品溯源场景的优化 PBFT 算法——t-PBFT 算法。t-PBFT 算法将供应链中的节点划分为 3 个等级，根据这些节点在共识过程中的实际通信量来评价其的可靠性。此外，t-PBFT 算法简化了一致性协议的执行流程，降低了通信开销，提升了节点的共识效率。最后，基于 t-PBFT 算法并结合区块链技术提出一种满足食品溯源业务需求的系统架构模型，在后续的工作中将进一步研究该系统模型，减小算法与食品溯源实际应用中的相关差异，增强算法的适用性。

参 考 文 献

[1] NAKAMOTO S. Bitcoin: A peer-to-peer electronic cashsystem [EB/OL]. https://bitcoin.org/en/bitcoin-paper. 2008.

[2] YUAN Y, WANG F Y. The development and prospect of blockchain technology[J]. Acta Automatica Sinica, 2016, 42(4): 481-494.

[3] MARTEN R, KAI S. A blockchain research framework[J]. Business & Information Systems Engineering, 2017, 59(6): 385-409.

[4] MARCO L, LAKHANI K R. The truth about blockchain [J]. Harvard Business Review, 2017, 95(1): 118-127.

[5] ZOU J, ZHANG H N, TANG Y. Blockchain Technology Guide [M]. Beijing: Mechanical Industry Press, 2018: 158-161.

[6] HE Z. Information Integration of Cluster Supply Chain Based on Web Services[J]. Laboratory Research and Exploration, 2015, 34(1): 107-112.

[7] LIAO Q W. Research on Commodity Traceability Scheme Based on Blockchain Technology[D]. Guangzhou: South China University of Technology, 2018: 6-13.

[8] LI B D, YE C M. Blockchain-based automotive supply chain product traceability system[J]. Computer Engineering and Application, 2020, 56(24): 35-42.

[9] YU Z, GUO C, XIE Y B. Research on Medicine Anti-counterfeiting Traceability System Based on Blockchain[J]. Computer Engineering and Applications, 2020, 56(3): 35-41.

[10] WANG Z H, LIU P Z, SONG C B. Research on the flexible and trusted traceability system of agricultural products based on blockchain[J]. Computer Engineering, 2020, 46(12): 313-320.

[11] WANG W B, HOANG D T, HU P Z, et al. A survey on consensus mechanisms and mining management in blockchain networks [J]. IEEE Access, 2019, 7: 22328-22370.

[12] ZHANG L, LIU B X, ZHANG R Y. Overview of Blockchain Technology[J]. Computer Engineering, 2019, 45(5): 1-12.

[13] ONGARO D, OUSTERHOUT J. In search of an understandable consensus algorithm [C] // Proceedings of the 2014 USENIX Annual Technical Conference. Philadelphia, PA, USA, 2014: 305-319.

[14] CASTRO M, LISKOV B. Practical Byzantine fault tolerance[J]. OSDI, 1999, 20(4): 173-186.

[15] ZHANG C, WANG R, TSAIW T, et al. Actor-based Model for Concurrent Byzantine Fault-tolerant Algorithm [C] // 2019 International Conference on Computer, Network, Communication and Information Systems (CNCI 2019). At lantis Press: IEEE, 2019: 552-555.

[16] LAMPORT L, SHOSTAK R, PEASE M. The byzantine general's problem[J]. ACM Transactions on Programming Languages and Systems, 1982, 4(3): 382-401.

[17] WANG Y H, CAI S B, LIN C L, et al. Study of blockchains's consensus mechanism based on credit[C] // IEEE Access. 2019: 10224-10231.

LI Bo, born in 1996, postgraduate. His main research interests include blockchain technology and consensus algorithm.

XIANG Hai-yun, born in 1982, postgraduate. His main research interests include information management technology and blockchain technology.