文章编号:1671-4598(2024)06-0220-07 DOI:10.16526/j.cnki.11-4762/tp.2024.06.032 中图分类号:TP391.1 文献标识码:A

基于区块链溯源的包装防伪信息追溯方法

李 峰
(海南天鉴防伪科技有限公司,海口 570314)

摘要:针对假冒伪劣产品日益增多,给消费者和厂家带来了极大的信任危机的问题,提出基于区块链溯源的包装防伪信息追溯方法,该方法利用区块链技术的不可篡改性、分布式共识和透明性,实现了商品生命周期的全程可追溯和防伪保障;为了验证该方法的可行性和效果,进行了一系列仿真实验,通过对各个参数进行设置,并对算法进行了不同性能指标的测试,最后对实验进行了分析和讨论;实验结果表明,优化后的算法在通信成本、吞吐量和延迟3个方面比PBFT效果优异,采用优化算法的包装防伪信息追溯方法能够有效地防止假冒伪劣产品的流通,提升消费者对产品的信任度;通过进一步的研究和实践,可以优化该方法,为推动商业生态系统的可持续发展提供了一定的理论基础。

关键词:区块链;包装防伪溯源;共识算法;联盟链;阈值签名

Packaging Anti-counterfeiting Information Traceability Method Based on Blockchain Traceability

LI Feng
(Hainan Tianjian Anti Counterfeit Technology Co., Ltd., Haikou 570314, China)

Abstract: In response to the increasing number of counterfeit and shoddy products, it brings a great crisis of trust to consumers and manufacturers, a packaging anti-counterfeiting information traceability method based on blockchain traceability is proposed. This method utilizes the immutable, distributed consensus and transparency of blockchain technology to realize the full traceability and anti-counterfeiting protection of the commodity life cycle. In order to verify the feasibility and effect of the method, a series of simulation experiments are carried out, through the setting of each parameter, the different performance indicators of the algorithm are tested, finally, the experiment is analyzed and discussed. The experimental results show that the optimized algorithm is superior to the practical byzantine fault tolerance (PBFT) in three aspects of communication cost, throughput and delay. The optimized packaging anti-counterfeiting information tracing method can effectively prevent the circulation of fake and shoddy products and improve consumers' trust in products. Through further research and practice, the method can be optimized, which provides a theoretical basis for promoting the sustainable development of business ecosystem.

Keywords: blockchain; packaging anti-counterfeiting traceability; consensus algorithm; alliance chain; threshold signature

0 引言

在过去的几年里,伪劣商品问题已经成为全球范围内一个严重的问题,这不仅损害了消费者的权益,还对企业的品牌形象和市场竞争力造成了巨大影响。为了应对这一挑战,各行各业纷纷寻求有效的防伪溯源技术。传统的防伪技术,如水印、激光防伪等,虽然在一定程度上起到了作用,但仍然存在诸多局限性,如易被仿冒、信息不透明等。因此,寻求一种更加安全、可靠且透明防伪溯源技术迫在眉睫。

近年来,区块链技术凭借去中心化、不可篡改和安全性等特点,逐渐成了防伪溯源领域的研究热点。区块链技术可以将产品的生产、流通、销售等关键信息记录在一个去中心化的、公开透明的数据库中,从而确保数据的真实性和完整性。国内外学者对此也有许多研究,文献[1]在分析区块链原理之后提出一种基于区块链的化妆品防伪溯源方案,利用已有的开放联盟链构建区块链防伪溯源监管平台,以此来满足化妆品的防伪溯源需求,但是该方案成本较高且用户隐私不能受到保护,仍存在被网络攻击的风险。

收稿日期:2023-06-16; **修回日期**:2023-07-16。
基金项目:海南省重大科技计划项目(ZDKJ2021047)。
作者简介:李 峰(1963-),男,大学本科,高级工程师。
引用格式:李 峰.基于区块链溯源的包装防伪信息追溯方法[J].计算机测量与控制,2024,32(6):220-226.

文献［2］在对区块链和无线通信技术（RFID，radio frequency identification）进行研究分析的基础上，提出了一种基于区块链和 PFID 技术的酒类防伪溯源系统。系统采用 RFID 标签和读写器作为上位机的传感器，区块链和 Web 端口作为下位机的传感器。经测试，该系统能够满足酒类信息的防伪溯源，但在平台设计方面并不完整，仍然需要优化。另外在人机交互方面还需要进行改进，系统性能也有待提高。

针对以上问题，该方法旨在探讨基于区块链源的包装防伪信息追溯方法，分析区块链的原理和拜占庭容错算法（PBFT，practical byzantine fault tolerance）可扩展性优化算法，然后构建利用现有溯源系统耦合区块链技术的包装防伪信息追溯方法。

1　区块链技术原理

区块链技术是一种去中心化、不可篡改的分布式账本技术，最早提出区块链技术概念是比特币的创始人中本聪，他在 2008 年 11 月发布的《比特币：一种点对点的电子现金技术》一文中首次提出了区块链的概念。随着时间的推移，区块链技术得到了越来越多人的关注和应用，并在各个领域展现了巨大的潜力。

区块链的核心特点包括去中心化、安全性、透明性和可追溯性。它通过将数据以区块的形式进行链式连接，使得任何参与者都可以验证和存储交易或数据记录，从而实现了无需信任第三方的可靠性。

1.1　区块链的结构和工作原理

区块链的结构是由多个区块组成的链式结构，每个区块包含一组交易和其他相关信息，并通过加密哈希值实现区块之间的链接。区块链技术提供了一个去中心化、开放的、拜占庭容错的交易机制，有望成为下一代互联网交易的基础框架。区块通常包括区块头、交易数据、当前区块哈希值、前一区块哈希值和随机数，彼此按照时间顺序连接成链，确保了数据的顺序和完整性，其区块结构如图 1 所示。

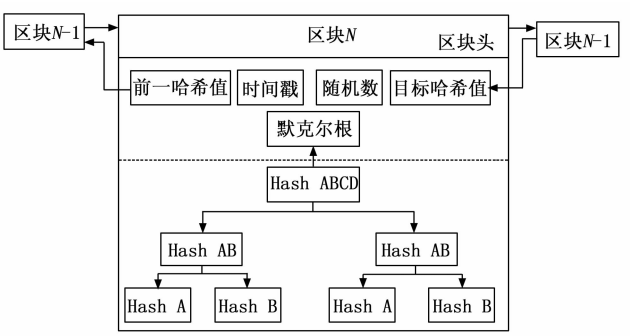


图 1　区块结构示意图

由图 1 可知，区块链的工作原理可以分为数据记录、哈希值链接、共识达成和区块链扩展 4 个步骤。通过区块链的数据结构和工作原理，可以实现分布式、去中心化的数据存储和传输[3]。这种工作原理使得区块链成为一种透明、可信的信息存储和传输环境，为基于区块链的包装防伪信息追溯方法提供了可靠的基础。

1.2　区块链的分类

在实际应用中，区块链多分为公有链、私有链和联盟链，私有链和联盟链的兴起源于使用群体的需求。其具体区块链的分类如表 1 所示。

表 1　区块链的分类

类别	公有链	私有链	联盟链
参与者	任何人	个体	联盟成员
记账者	所有节点	自定义	特定节点
算法	PoW	RAFT	PBFT
中心化程度	去中心化	可以完全去中心化	多中心化
激励机制	需要	可选	可多种
吞吐量	多	少	较少
能源消耗	大	小	较小

公有链是一种开放的、去中心化的区块链网络，任何人都可以加入并参与其中。每个人都可以成为节点，每笔交易都可以公开验证，数据也是公开透明的。比特币和以太坊是两个知名的公有链，也是区块链的著名应用。

私有链也被称为专有链，是一种基于区块链技术的封闭网络，特定的参与者被授权加入一个封闭网络中，但是这些数据和交易通常对外部参与者不可见，只有授权的节点才能验证和记录这些交易。这些节点通常是在该区块链中唯一被授权加入该网络的，或者是由单个组织或企业控制管理。因为私有链严格控制节点的加入，所以一般不存在恶意节点。

联盟链是由多个组织或实体，通过一个共同达成一致的方式，形成一个半中心化区块链网络，在联盟链中，参与各方之间通过共识协议实现共识，并且在一定程度上共享对交易的控制权。联盟链的核心在于多个组织或实体之间基于一套共识协议实现共识，在这些组织或实体中，参与者通过共同达成一致来管理和维护联盟链[4]。由于联盟链通常具有更高的性能和可扩展性，并且在某些情况下还提供一定程度的隐私性。因此，在不同领域中，联盟链广泛应用于跨组织合作、供应链管理和金融领域等。

这些不同类型的区块链网络适用于不同的应用场景和需求。公有链强调去中心化、公开和透明，私有链注重安全性和控制性，而联盟链提供了中间地带，平衡了安全性、可控性和性能等因素。

1.3　区块链共识算法概述

比特币的出现不仅解决了在去信任化的点对点网络中实现价值转移的问题，而且其采用的 PoW 共识算法联合经济激励机制、密码学等使得区块链跨越了分布式系统中

拜占庭荣错这一鸿沟，给如何在分布式场景下达成共识带来了巨大的创新和突破。区块链时代自此到来，许多新的具有拜占庭容错性质的共识算法受比特币启发而陆续产生。

1.3.1 PoW

PoW 算法即工作量算法，适用于比特币系统的共识算法，其优点是完全去中心化，节点自由进出。通过设计与引入分布式网络节点的算法竞争，保证数据一致性和共识，PoW 算法也成了目前最广泛应用的区块链共识算法。

公有链中主要使用概率算法（POW，proof of work）。在生成区块时，PoW 算法会使节点计算随机值 nonce，该值要满足式（1）：

$$h(nonce \mid d \parallel) \leqslant t \tag{1}$$

式中，h 是哈希函数，d 是区块头中的元数据，t 是目标难度值。*nonce* 使区块头的元数据哈希值小于难度值 t，区块头的元数据包括上一区块哈希值、默克尔根和时间戳等。求解式（1）得出区块的记账权，且哈希函数一般为散列函数，求解过程只能用穷举法，该过程被称为“挖矿”。

然而，PoW 算法也存在一些问题。首先，它需要大量的能源消耗，因为计算密集型任务需要大量的电力支持，所以它不会造成任何经济损失。其次，由于竞争激烈，矿工们需要不断更新他们的硬件设备，这导致了计算设备的不断更新和资源浪费[5]。最后，PoW 算法对于可扩展性有一定的限制，因为随着参与者数量的增加，网络的吞吐量可能会下降。

1.3.2 RAFT

在私有链中，通常的共识算法就是传统的分布式共识算法，也就是 RAFT 算法。与传统的分布式共识算法不同，RAFT 算法的设计目标是提供一个可理解的共识算法，使得开发者更容易理解和实现分布式系统。与传统的分布式共识算法（如 Paxos）相比，RAFT 算法的设计更加模块化，将共识问题分解为几个相对独立的子问题，比如数据同步、数据加载、一致性检查等。

RAFT 算法的核心概念包括领导者、跟随者和候选人，其 RAFT 选举过程如图 2 所示。

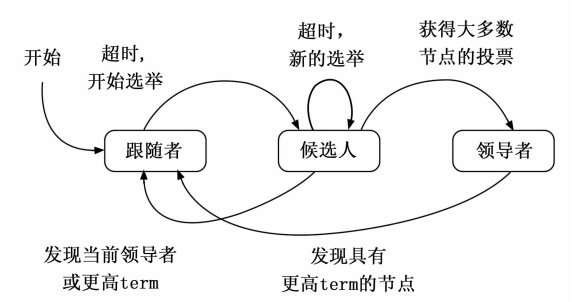


图 2 RAFT 选举过程

每个节点都有一个随机的选举超时时间。该时间决定了一个节点是否能在一定的时间内收到来自前领导者的信息。如果一个节点在一定时间内没有接收到来自领导者的消息，它就会假设当前领导者失去联系，并触发选举过程。在这种情况下，当一个节点成为候选人后，它向其他节点发送选举请求。如果候选人收到了大多数节点的投票，它就成为新的领导者[6]。否则，如果在选举期间出现了新的领导者，候选人会回到跟随者状态。一旦领导者选举完成，它就可以接收客户端的操作请求，并将操作作为日志条目追加到自己的日志中。领导者通过发送附带日志条目的心跳消息来复制日志到其他节点。一旦节点确认接收到日志条目，它们就会将其应用到自己的状态机中，实现一致的状态。

RAFT 算法通过领导者选举和日志复制机制来确保分布式系统的一致性和可用性。它的设计简洁明了，易于理解和实现，使得开发者能够更好地构建可靠的分布式系统。

1.3.3 PBFT

实用拜占庭容错算法（PBFT，practical byzantine fault tolerance）出现，使得拜占庭协议的运行复杂度从指数级别降低到多项式级别，保证了算法的活跃性和安全性。在联盟链中，通常使用能耗小的 PBFT 算法。PBFT 中参与共识的节点是复制节点，节点分为主节点与备份节点。主节点负责接收客户的请求，并组播给其他备份节点。其运行 PBFT 共识流程如图 3 所示。

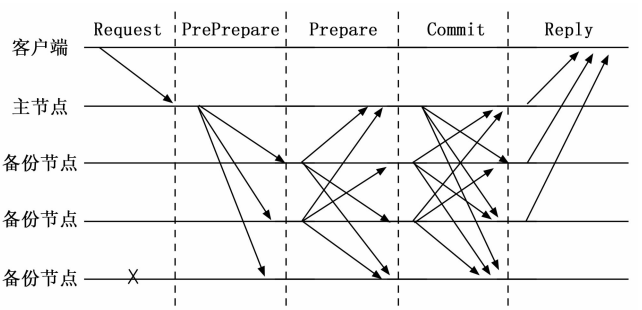


图 3 PBFT 共识流程

在图 3 中，主节点在预备（PrePrepare）阶段对客户端进行验证，然后将收到的请求广播给所有副本节点，并生成一个唯一的序列号。节点在准备（Prepare）和提交（Commit）收到足够数量的预备消息后，发送准备消息来表明它们已经达成共识，准备消息包含预备消息的摘要。在响应（Reply）阶段将执行结果回复到客户端。

PBFT 算法通过多个阶段的消息交互和多个节点的验证和确认，达成在拜占庭容错环境下的共识。它可以容忍少数节点的恶意行为或故障，并确保系统的一致性[7]。然而，现有的 PBFT 共识算法存在着一些不足，主节点的选取方式较为随意，不能保证主节点的最优性，PBFT 算法的消息传递和验证过程比较复杂，它在性能和可扩展性方面可能会受到一些限制。

2 基于阈值签名的 PBFT 可扩展性算法优化

TBFT 是基于阈值签名的 PBFT 扩展性改进的共识算

法，可以在 BFT 节点数小于总数 1/3 的情况下，保证系统的安全运行。其 TBFT 共识算法结构如图 4 所示。

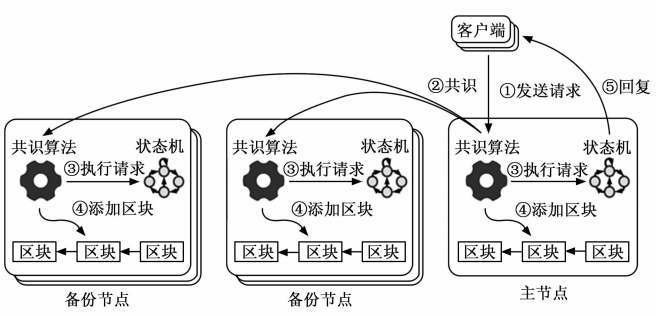


图 4　TBFT 共识算法架构图

在图 4 中，TBFT 分为主节点和备份节点。主节点接受请求提出新的数据块，开始 TBFT 共识，在共识过程中，通过阈值签名技术优化了准备和提交阶段，然后聚合签名，将信息发送到主节点。主节点收到共识结果后执行客户端请求，并回复结果给客户端[8]。在回应阶段，TBFT 通过默克尔根将接受信息数降低到 1，以此确保所有正常节点以相同顺序执行相同操作。

TBFT 采用基于 BLS 签名的阈值签名方案。在整个设计中，要先用密钥生成函数 GenKeys，计算公式见式（2）：

$$pk_i = sk_i \times G \tag{2}$$

式中，pk_i 是节点 i 对应的公钥，sk_i 是节点 i 随机生成的私钥，G 是阶乘法循环群的生成元。再得出公钥之后要进行广播，并计算出聚合公钥 P，计算公式见式（3）：

$$P = a_1 \cdot pk_1 + a_2 \cdot pk_2 + \cdots + a_n \cdot pk_n \tag{3}$$

式中，a_i 是非线性系数，起到保护密钥防止攻击的作用，节点广播对 pk_i 的签名来验证式（3）中聚合公钥 P 的正确性。通过节点 i 对其余节点签名 pk_i 的收集，可以得出成员密钥 MK_i，计算公式见式（4）：

$$MK_i = (a_1 \cdot sk_1) \times H(pk_1) + \cdots + (a_n \cdot sk_n) \times H(pk_n) \tag{4}$$

式中，MK_i 是成员密钥，sk_i 是私钥，H 是曲线哈希函数，pk_i 是公钥，MK_i 是对 $H(pk_i)$ 的多重签名。

节点在接收到信息 m 后，通过计算得出信息的摘要（d），在此基础上，根据私钥 sk_i 和成员密钥 MK_i 计算出签名 S_i，计算公式见式（5）：

$$\begin{cases} d = h(m) \\ S_i = sk_i \times H(d) + MK_i \end{cases} \tag{5}$$

式中，h 是加密散列函数，$H(d)$ 是摘要的曲线哈希函数。签名 S_i 通过节点 i 进行广播，并对其余签名进行收集，得出聚合公钥 S，计算公式见式（6）：

$$S = \sum_{i=1}^{k} (sk_i \times H(d) + MK_i) \tag{6}$$

式中，$H(d)$ 是摘要的曲线哈希函数，sk_i 是私钥，MK_i 是成员密钥。得出聚合签名 S 要对其进行正确性验证，验证公式见式（7）：

$$e(G,S) = e[P', H(d)] \cdot e[P, H(pk_1) + \cdots + H(pk_n)] \tag{7}$$

式中，G 是阶乘法循环群的生成元，S 是聚合签名，P' 是 n 个节点的聚合公钥。

TBFT 算法的共识流程包括 Request 阶段、Propose 阶段、Propose-Sign 阶段、Prepare 阶段、Prepare-Sign 阶段、Commit 阶段和 Reply 阶段。其 TBFT 算法流程如图 5 所示。

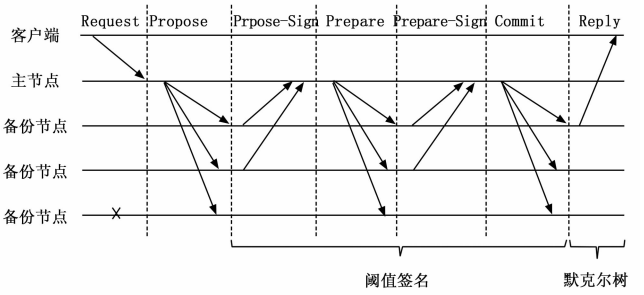


图 5　TBFT 算法共识流程图

由图 5 可知，Propose 阶段和 Prepare 阶段的节点请求顺序在同一个视图中保持一致，Propose 阶段和 Commit 阶段的请求在不同视图之间严格排序。在共识流程中，主节点生成一个新的序列号，并将请求、序列号和视图编号打包成预准备消息，然后广播给所有副本节点。副本节点向所有节点发送提交消息，包含自己的节点 ID、视图编号、序列号和请求的摘要。副本节点收到提交消息后，验证消息的合法性，如果验证通过，则将提交消息存入日志[9]。副本节点执行请求后，生成结果，并将结果、视图编号、序列号和自己的节点 ID 打包成回复消息，然后发送给客户端。客户端收到回复消息后，验证消息的合法性，如果验证通过，则接受结果。

在 TBFT 中，阈值签名技术被用于准备阶段和提交阶段，以减少网络通信的开销。具体来说，副本节点在发送准备消息和提交消息时，不再向所有节点发送，而是只向部分节点发送[10]。这部分节点被称为委员会（Committee）。委员会的大小是可配置的，通常大于 2，以保证系统的安全性和灵活性。

3　基于区块链溯源的包装防伪信息追溯方法

结合该方法提出的基于阈值签名的 PBFT 可扩展性优化算法以及现有的防伪溯源系统，提出了一种基于区块链溯源的包装防伪信息追溯方法。在建立系统之前，需要明确供应链的基本流程，然后依据供应链网络中处于不同角色位置的用户需求，对溯源系统所需要的功能进行分析。首先，该方法面向厂家、销售商和消费者，可以建立可信的、不可篡改的信息溯源系统，以确保产品的真实性和合规性。同时，该方法适用于各类包装。在具体实施中，应用该方法提出的包装防伪信息追溯方法时，商品包装上会

印有一个二维码，该二维码可以实现对商品生命周期的全程追踪和记录。在该系统中，通过将防伪溯源与区块链技术相结合，企业可以实现对商品从原材料采购到生产过程以及物流运输等环节的全流程追溯和记录，以此帮助企业提升产品质量管理和追溯能力，减少产品质量问题的发生[11]。

该方法设计基于区块链 PBFT 共识算法的防伪溯源系统，其方案设计原理如图 6 所示。

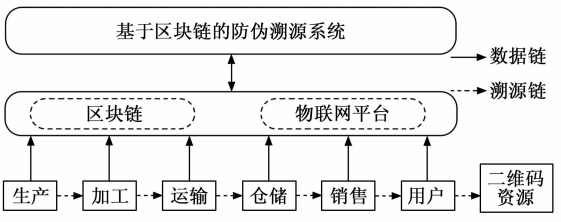


图 6 方案设计原理图

由图 6 可知，商品的生产、加工、运输、仓储环节通过物联网设备获取所需要的信息，然后通过传输协议将信息上传到云端物联网平台，组成商品在销售前的包装上的溯源信息。然后在商品的销售阶段，销售商和顾客可以通过扫二维码对商品进行溯源[12]。

商品的溯源数据永久储存在区块链中，区块链确保信息不可篡改，保证了产品的真实性，在整个方法中，每一环节的数据都具有唯一性且不可造假，遇到数据不一致的情况，只需将数据与云端储存的溯源数据进行对比，即可定位到数据冲突环节，对其进行追责。

基于区块链溯源的包装防伪信息追溯系统的架构如图 7 所示。

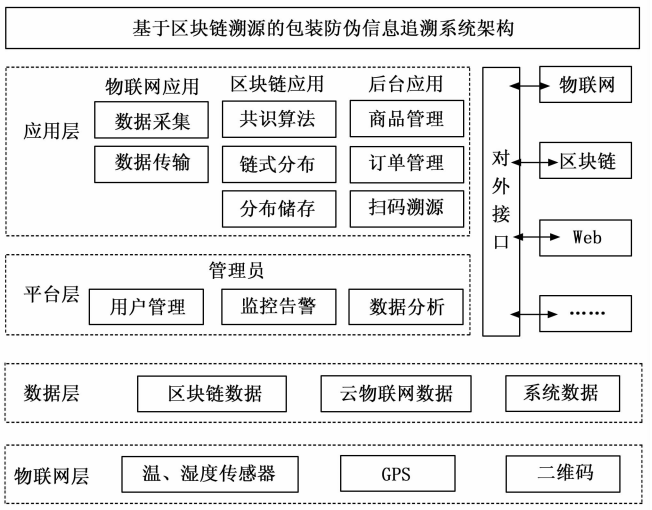


图 7 系统架构图

由图 7 可知，系统架构分为 5 层，分别是应用层、平台层、数据层、物联网层和对外接口。

1）物联网层通过温度传感器、湿度传感器和 GPS 收集商品信息，信息构成溯源数据[13]，在商品包装上贴有一个包含溯源信息数据的二维码，可以扫码溯源。

2）数据层包括区块链数据、云物联网数据和系统数据。区块链用来储存商品溯源数据，该数据具有唯一性；物联网数据是指通过物联网层采集到的商品信息，将其储存在云端；系统数据主要指用户数据，方便与区块链中的商品溯源数据进行对比。

3）平台层指的是系统管理员，其可以对用户进行管理，在发现商品信息与溯源数据不符时进行监控告警，同时要对数据进行分析，通过 ECHarts 对共识算法数据进行展示[14]。

应用层包括物联网应用、区块链应用和后台应用，物联网应用即将采集到的数据进行上传，区块链应用是指通过算法对用户的请求进行共识，利用分布式存储方便储存商品溯源数据，后台应用指的是对商品进行管理，运输商通过后台进行运输管理，最终达到扫码溯源的目的。

4 实验分析

该方法提出了一种在已有溯源系统的前提下，耦合区块链 PBFT 可扩展性优化算法的包装防伪信息追溯方法[15]。为了验证该方法的可行性，需要对区块链 PBFT 可扩展性优化算法进行实验分析，即分别从通信成本、吞吐量和延迟 3 个方面对优化算法和 PBFT 对比分析。

4.1 实验设置

优化算法测试系统由 4 个部分组成，分别是数据层、通信层、网络层和共识算法层。其中，数据层由各种类型的传感器以及输入数据都会被用于实现算法；通信层由各个不同的通信节点构成，用于实现数据的传递和处理；网络层则是利用 Google 的反射机制，通过模拟不同类型的网络节点实现通信；共识算法层主要针对 3 个方面进行仿真测试，即通信成本、吞吐量、延迟。测试设备配备英特尔酷睿 i7（2.2 GHz）CPU、双 16 G 内存条和 Windows 操作系统。

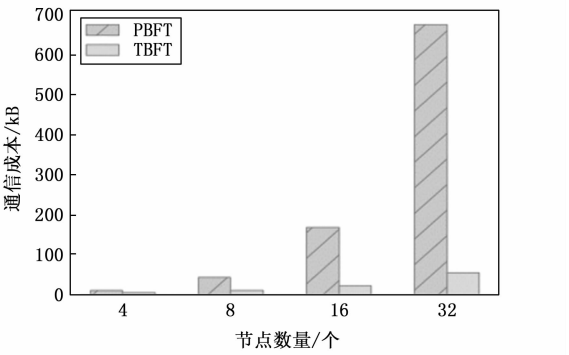
4.2 通信成本分析

通信成本分析基于区块链网络请求共识产生的消息量和消息大小，优化算法和 PBFT 通信成本对比如图 8 所示。

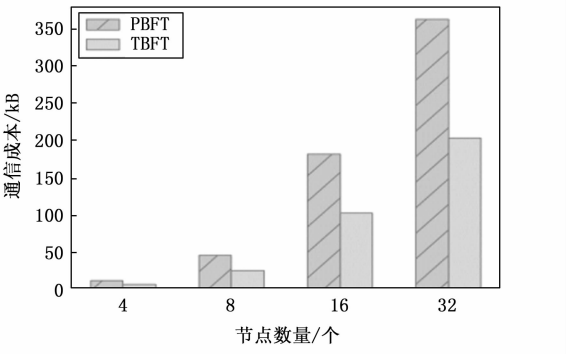
从图 8（a）中可以看出，随着节点数量的增加，优化算法和 PBFT 的成本差距越来越大。当节点数量为 8 时，优化算法的通信成本是 12 kB，PBFT 的通信成本是 44 kB；在节点数量为 32 时，优化算法的通信成本是 55 kB，PBFT 的通信成本是 673 kB，优化算法的通信成本仅为 PBFT 的 8.17%。从图 8（b）中可以看出，在相同请求数量下，优化算法的通信成本都要低于 PBFT 的通信成本。综上所述，优化算法在通信成本方面要小于 PBFT。

4.3 吞吐量分析

吞吐量代表一个系统在单位时间内处理事务的能力，随着每个区块的容量增加，吞吐量也相应地增大，共识时



（a）不同节点数量下的通信成本



（b）不同请求数量下的通信成本

图 8　优化算法和 PBFT 通信成本对比

延和网络负载也会增加，因此当区块容量大到一定程度时吞吐量有所下降利用优化算法和 PBFT 处理大小固定为 1 MB、请求为 250 B 的区块，其优化算法和 PBFT 吞吐量对比如图 9 所示。

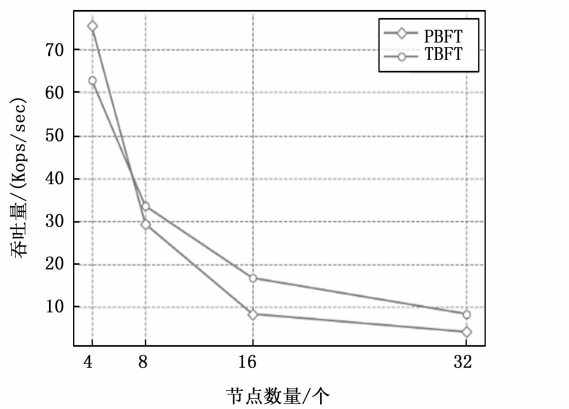
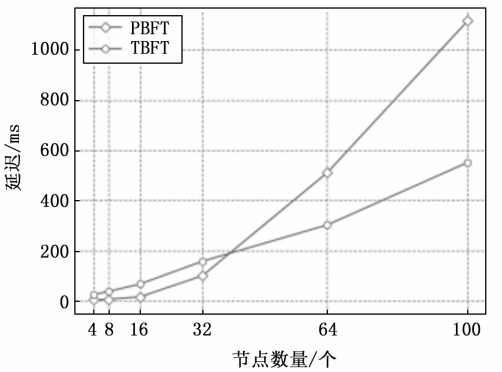


图 9　优化算法和 PBFT 吞吐量对比

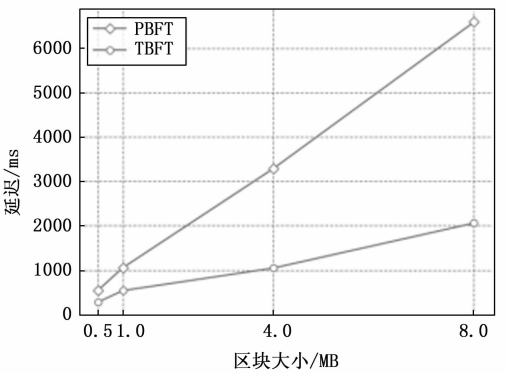
从图 9 中可以看出，随着节点总数的增加，这两种算法都有略微的下降，当节点数为 6 时，优化算法和 PBFT 的吞吐量一致；节点数小于 6 时，优化算法的吞吐量低于 PBFT 的吞吐量；节点数大于 6 时，优化算法的吞吐量大于 PBFT 的吞吐量。在节点数为 16 时，优化算法的处理速度高达每秒 16 000 客户端请求，而 PBFT 的处理速度仅有每秒 8 000 客户端请求[17-18]。综上所述，在节点数大于 6 时，随着节点的增加，优化算法在吞吐量方面高于 PBFT。

4.4　延迟分析

在对优化算法和 PBFT 进行延迟分析时，为了减少误差的影响，结果采用 100 次实验的平均值，其优化算法和 PBFT 的延迟对比如图 10 所示。



（a）不同节点数量下的延迟



（b）不同区块大小下的延迟

图 10　优化算法和 PBFT 的延迟对比

从图 10（a）中可以看出，节点数小于 32 时，优化算法处理请求的延迟要高于 PBFT，但是 PBFT 的延迟在节点数大于 32 时呈指数增长[19-20]。当节点数为 64 时，优化算法的延迟是 300 ms，PBFT 的延迟是 510 ms，而当节点数为 100 时，优化算法的延迟是 550 ms，PBFT 的延迟高达 1 150 ms。

从图 10（b）中可以看出，区块越大，优化算法的延迟比 PBFT 越小。总之，节点数量增加和区块大小增加的情况下，优化算法在延迟方面要低于 PBFT[21]。

在对通信成本、吞吐量和延迟分别进行对比分析之后，优化算法的效果要好于 PBFT，可以得出该方法提出的方法具有较好的使用效果。

5　结束语

该方法提出一种基于区块链 PBFT 可扩展性优化算法的包装防伪信息追溯方法，通过利用区块链技术的不可篡改性、分布式共识和透明性，可以实现商品周期的全程可追溯和防伪保障。这种方法为消费者提供了一个可信的途

径来验证产品的真实性和合规性。消费者扫二维码获取商品的生产、加工、运输、仓储和销售环节信息，这样的透明度和可追溯性有助于减少假冒伪劣产品的流通，保护消费者的权益。

仿真实验表明，该方法采用的优化算法在通信成本、吞吐量和延迟 3 个方面比 PBFT 的表现更好，基于此优化算法的包装防伪溯源方法，有着较强的实用性和可靠性。但是该方法实验部分并未真正应用到实际生活中，其结果偏理想化，后续对其技术简化后进行大规模普及。

参考文献：

[1] 杨皓然，杨绮鹏. 基于区块链的化妆品防伪溯源方案 [J]. 信息与电脑（理论版），2022，34 (24)：46 - 49.

[2] 王黎亚，谢祖光，李海峰，等. 区块链技术在烟草溯源和防伪中的应用 [J]. 企业科技与发展，2021，47 (1)：41 - 42.

[3] 王建涛，黄昕锐，薛　亮，等. “区块链＋溯源”防伪系统综述 [J]. 信息与电脑（理论版），2022，34 (8)：15 - 19.

[4] 孙嘉慧. 基于区块链的防伪溯源技术研究与系统实现 [D]. 北京：北京邮电大学，2020.

[5] HUANG L，ZHANG G，YU S，et al. SeShare：Secure cloud data sharing based on blockchain and public auditing [J]. Concurrency and Computation：Practice and Experience，2019，31 (22) 1 - 15.

[6] 孙伟容. 基于区块链和 RFID 技术的酒类防伪溯源系统研究 [D]. 南京：南京理工大学，2021.

[7] KAMILARIS A，FONTS A，PRENAFETA-BOLDU F X. The rise of blockchain technology in agriculture and food supply chains [J]. Trends in Food Science & Technology，2019，91：640 - 652.

[8] 林　契. 基于区块链的物联网安全技术探究 [J]. 信息与电脑（理论版），2019，425 (7)：165 - 166.

[9] 丁庆洋，朱建明. 区块链视角下的 B2C 电商平台产品信息追溯和防伪模型 [J]. 中国流通经济，2017，31 (12)：41 - 49.

[10] 何宏浩. 区块链上基于所有权的溯源防伪系统的设计与实现 [D]. 杭州：浙江工商大学，2019.

[11] 金　鹏，薛哲彬，江润恬，等. 基于区块链技术的服装可追溯系统设计与实现 [J]. 丝绸，2021，58 (5)：62 - 69.

[12] 梁晓颖，王利君. 基于区块链技术的服装供应链研究 [J]. 毛纺科技，2020，48 (3)：65 - 70.

[13] 陈思源，崔子杰，刘丹飞，等. 区块链在产品溯源和包装防伪上的应用进展 [J]. 包装工程，2023，44 (1)：91 - 100.

[14] 鲁　意. 区块链 PBFT 共识算法的可扩展性优化研究与实现 [D]. 南京：南京邮电大学，2022.

[15] 薛中伟. 基于区块链技术的工控数据安全传输系统设计 [J]. 计算机测量与控制，2022，30 (4)：161 - 164.

[16] 熊　琎. 基于区块链技术的网络安全漏洞检测系统设计 [J]. 计算机测量与控制，2021，29 (5)：59 - 63.

[17] 刘佳宝. 基于一致性共识算法的区块链技术在物流信息平台的应用 [D]. 太原：太原师范学院，2023.

[18] 谭朋柳，王润庶，曾文豪，等. 区块链共识算法综述 [J]. 计算机科学，2023，50 (s1)：691 - 702.

[19] 刘　峰，王一帆，杨　杰，等. 一种基于区块链的融合 DKG 与 BLS 的高阈值签名协议 [J]. 计算机科学，2021，48 (11)：46 - 53.

[20] 郭垚垚. 区块链共识算法研究与实现 [D]. 北京：北京邮电大学，2021.

[21] 陈冠瑜. 区块链视角下物流信息平台的改进研究 [D]. 太原：山西财经大学，2023.

（上接第 197 页）

[15] WOO S，PARK J，LEE J Y，et al. CBAM：convolutional block attention module [C] //Proceedings of the 15th European Conference on Computer Vision. Munich：Springer，2018：3 - 19.

[16] HU J，SHEN L，SUN G. Squeeze-and-excitation networks [C] //IEEE/CVF Conference on Computer Vision and Pattern Recognition. Salt Lake City，USA：IEEE，2018：7132 - 7141.

[17] WANG Q，WU B，ZHU P，et al. ECA-Net：efficient channel attention for deep convolutional neural networks [C] //2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)，2020：11531 - 11539.

[18] WANG J，XU C，YANG W，et al. A normalized Gaussian Wasserstein distance for tiny object detection [J]. Arxiv Preprint，2022：6 - 14. Arxiv：2110. 13389.

[19] MA N N，ZHANG X Y，ZHENG H T，et al. ShuffleNet V2：practical guidelines for efficient CNN architecture design [C] //Computer Vision-ECCV 2018. Lecture Notes in Computer Science. Cham：Springer，2018：122 - 138.

[20] BISWAS D，SU H，WANG C，et al. An automatic traffic density estimation using single shot detection (SSD) and MobileNet-SSD [J]. Physics and Chemistry of the Earth，2019，110：176 - 184.

[21] HAN K，WANG Y H，TIAN Q，et al. GhostNet：more features from cheap operations [C] //Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Seattle，2020：1577 - 1586.

[22] LI H，LI J，WEI H，et al. Slim-neck by GSConv：A better design paradigm of detector architectures for autonomous vehicles [J]. Computer Science，[2023-01-23]. DOI:10.48550/arXiv.2206.02424.