计算机应用研究
Application Research of Computers
ISSN 1001-3695,CN 51-1196/TP

《计算机应用研究》网络首发论文

题目：基于双区块链及物联网技术的防伪溯源系统
作者：李宣，柳毅
DOI：10.19734/j.issn.1001-3695.2019.08.0291
收稿日期：2019-08-08
网络首发日期：2020-01-09
引用格式：李宣，柳毅．基于双区块链及物联网技术的防伪溯源系统[J/OL]．计算机应用研究. https://doi.org/10.19734/j.issn.1001-3695.2019.08.0291

网络首发时间：2020-01-09 10:55:02
网络首发地址：http://kns.cnki.net/kcms/detail/51.1196.TP.20200108.1109.011.html

基于双区块链及物联网技术的防伪溯源系统 *

李 宣†，柳 毅

(广东工业大学 计算机学院，广州 510006)

摘 要：在产品安全日益重要的今天，传统的产品溯源系统依旧存在着中心化存储、数据可信度低、数据易窜改及责任人定位困难等问题。鉴于区块链技术能够凭借其分布式存储、链式结构、不可窜改和高容错性等特点，在信息的搜集、存储和共享等过程中实现数据溯源功能，并借助物联网技术保证区块链源头数据的真实可靠，实现对产品信息的实时跟踪。基于此，提出了使用双区块链和物联网技术的产品防伪溯源系统，分析了该溯源系统的安全性并通过仿真实验验证了该系统的可行性，对区块链技术和产品安全领域的进一步结合提供了参考和借鉴。

关键词：双区块链；溯源系统；物联网

中图分类号：TP391 doi: 10.19734/j.issn.1001-3695.2019.08.0291

Traceability system based on double blockchain and Internet of Things technology

Li Xuan†, Liu Yi

(*School of Computer*, *Guangdong University of Technology*, *Guangzhou* 510006, *China*)

Abstract: Nowadays, product safety is becoming more and more significant. There still exists some problems in traditional product traceability system, such as centralized storage, low data reliability, easy tampering of data and difficultly located responsible. By virtue of its traits of distributed storage, chain structure, non-tampering and high tolerance, blockchain can develop its function of information traceability in the process of information collection, storage and sharing. At the same time, it can ensure the reality of the source data of block chain by Internet of Things technology and realize the tracking of product information constantly. On this basis, this paper discussed the possibility of applying blockchain to product traceability, on this basis, a product security traceability system using dual blockchain and Internet of Things technology is proposed and The security and feasibility of traceability system have been testified by simulation experiments, which provide a reference for the further integration of block chain and product safety technology.

Key words: dual blockchain; traceability system; Internet of things

0 引言

食品安全关乎着每一个人。在过去数十年间，从地沟油、三聚氰胺奶粉到染色馒头、病死猪肉等食品安全事件，使得消费者已经丢失对食品安全的信心。为了使消费者重拾信心，产品信息溯源是食品安全管理的重要手段。我国二十年前就已提出产品安全溯源体系，然而未能实现全面有效的产品信息溯源。传统的产品溯源方法仍然面临着信息不对称、发生安全事故时责任人定位困难、产品溯源信息不可靠等诸多问题。区块链技术的出现，或许能给传统的产品信息溯源技术带来翻天覆地的变革。

区块链技术起源于 2008 年，由一位名叫 Satoshi Nakamoto 的学者在加密货币的奠基性文章《比特币：一种点对点电子现金系统》[1]中提出。其最初作为加密货币-比特币的底层支撑技术被人们所熟知，之后因其良好的分布式存储、数据可追溯、数据不可窜改以及去中心化等特性得到人们的认可，被认为是继大型机、个人电脑、互联网之后计算模式的颠覆式创新[2]。随着时间的推移，区块链技术不断完善，其应用场景也不再局限于加密货币，而是更多的应用在如电子投票[3]、医疗[4]、慈善[5]和分布式账本[6]等领域。可以预见的是，在不远的将来，区块链技术将会更加完善，其应用场景将会更加广泛。在区块链的诸多应用场景中，产品信息溯源[7]已经逐渐成为一种重要的应用场景。

目前已有一些基于区块链的产品溯源研究成果。文献[8]设计了一种基于区块链的去中心化数据溯源方法，避免数据窜改，实现数据的可信存储。文献[9]阐述了在供应链管理系统中融入区块链技术的可能，同时分析了二者结合时可能带来的一些问题。文献[10]设计了一个基于 RFID 和区块链技术的溯源系统 agri-food supply chain traceability system，以防止农产品溯源信息被窜改以及标签被复制，同时提出了 BigchainDB[11]的概念，用以解决区块链存储大数据时的性能问题。文献[12]设计了结合智能合约的 Eximchain，以此来管理供应链。文献[13]提出了一种基于区块链的葡萄酒供应链追溯系统，实现了从葡萄到酒瓶整个加工过程的公开透明。在双区块链的设计方面，刘家稷等[14]利用区块链的分布式存储、去中心化和不可窜改的特性设计了基于区块链技术的防伪溯源系统 TSPPB，使用公有链和私有链两层区块链，在确保溯源信息的真实可靠的同时，保证高效低成本的运行。但在整个系统的设计中，对监管部门的作用描述不清。丁庆洋等[7]使用双层架构提出了溯源许可链的共识机制，将参与者划分为两层，并在不同层上采用不同的共识机制，以此提高溯源系统的效率。但在设计过程中，没有考虑原始数据造假的可能性。

通过对相关文献的梳理可以发现基于区块链的溯源系统已有丰硕的成果，采用双区块链结构的方案也有文献涉及。但大多都关注于解决数据的不可窜改和去信任化，无法保证源头数据的真实可靠性，同时单单使用公有链或私有链，在效率方面又难以达到实际生产的要求。因此，本文结合区块

收稿日期：2019-08-08；**修回日期：**2019-09-24 **基金项目：**国家自然科学基金资助项目(61572144)

作者简介：李宣(1996-)，男(通信作者)，江西赣州人，硕士研究生，主要研究方向为区块链、信息安全(lx@mail2.gdut.edu.cn)；柳毅(1976-)，男，江苏连云港人，教授，博士，主要研究方向为网络与信息安全.

链的不可窜改、去中心化、分布式存储、信息可追溯等特点以及物联网技术针对产品性状实时跟踪的特性，提出基于双区块链及物联网技术的防伪溯源系统。

1　区块链技术

区块链是哈希函数、非对称加密技术、共识算法[15]及 P2P 网络等技术结合在一起形成的一种新型计算范式，是由多个称之为区块的数据结构链接而成的分布式数据库，并辅以密码学方式保证数据的不可窜改和不可伪造[16]。

如图 1 所示，区块链架构由上至下分为五层。其中，应用层代表了区块链的诸多应用场景，如产品溯源查询功能。激励层将经济因素融入到区块链技术中，如比特币和以太币中的出块奖励[1]机制。共识层中包含各种共识算法，使得区块链技术实现可编程的特性。网络层则包含着区块链技术的组网机制及验证机制。数据层封装了区块链存储的数据结构。

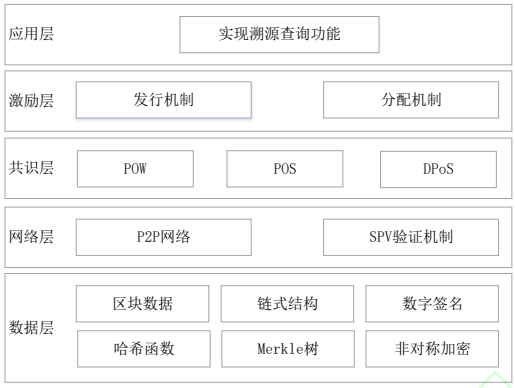

图 1　区块链技术架构

Fig. 1　Framework of the blockchain technology

1.1　区块链技术的特点

区块链得益与图 1 所示的五层技术架构，拥有以下三种重要特性：

a) 去中心化。即区块链能够在没有可信第三方背书的情况下完成数据的交互。如图 2 所示，区块链底层采用 P2P 网络架构，所有节点均能对等的与其他节点通信，随时随地查询数据，整个网络中不存在中心节点，实现了网络分布的去中心化、去信任化以及数据的公开透明。

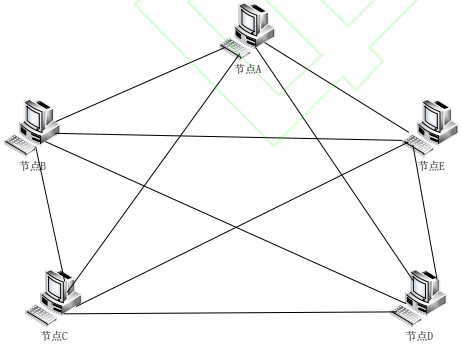

图 2　区块链分布式网络示意图

Fig. 2　Diagram of the blockchain distributed network

b) 不可窜改性。顾名思义，区块链上的数据是无法被窜改的。在区块链中，通过附加时间戳和区块间的链式连接以及哈希算法实现数据的不可窜改。如图 3 所示，每一个区块包含区块头和区块体。其中，区块头包含当前区块头哈希值、前一区块头哈希值、时间戳、区块难度和随机数等信息，区块体则包含当前区块的所有交易，区块头和区块体通过 Merkle tree[17]联系在一起。通过在每个区块中保存前一个区块的哈希值的方式，区块前后相连，形成链式结构。攻击者想要修改或添加某些数据项，势必会造成当前区块的哈希值变化，导致链式结构崩溃，大大增加了数据窜改的难度。同时，区块前后相连的特性，使得链上的任何数据都是可追溯的。因此，区块链中的数据具备安全性、不可窜改性及可追溯性。

c) 高容错性。区块链中的数据依靠共识机制保证所有节点的数据完整一致。所有节点都能参与共识，并且任何一小部分的节点损坏或离开都不会影响整个系统的稳定运行，针对单点故障[18]有天然的防范作用。

1.2　区块链的分类

根据应用场景的不同，区块链可以分为以下几种[19]：

a) 公有链：实现真正的去中心化结构，任何用户都可以加入区块链网络，生成新的交易或查看区块链信息。通过 POW(proof of work)、POS(proof of stake)、DPoS(delegated proof of stake)[20]等共识算法确认。

b) 私有链：私有链是在公有链的基础上，对加入权限增加限定，只有通过组织者授权的用户才能加入区块链网络中。一般私有链应用在企业中，提供安全、可追踪、自动化的平台[14]。

c) 联盟链：只有属于联盟的成员才能够生成交易或查看区块链信息，一般由多个企业或组织共同维护，为参与者提供认证、授权和管理等功能。

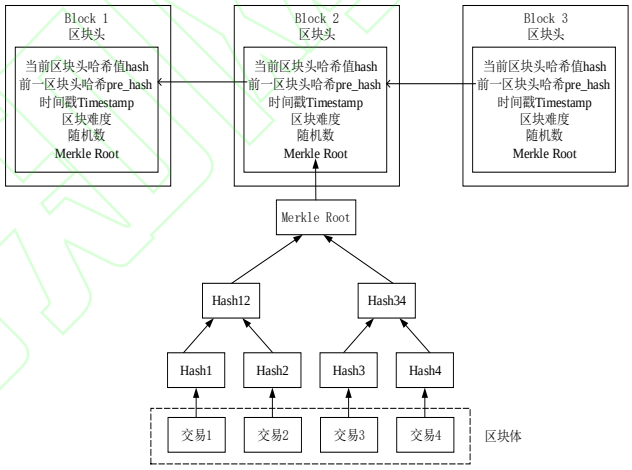

图 3　链式结构示意图

Fig. 3　Diagram of the blockchain structure

针对上述三种区块链，其特征对比如表 1 所示。公有链尽管没有权限限制，但能够实现去信任化。然而，因其参与人数众多，导致网络传输慢，存储效率低，不适合应用在拥有庞大数据的产品溯源系统中。私有链与联盟链本身包含权限限定，安全性优于公有链。同时，其存储效率高、吞吐量大，对大数据有较好的兼容性，适合在产品溯源系统中作为底层架构使用。

表 1　三种区块链特点对比

Tab. 1　Comparison of three blockchain characteristics

比较项	公有链	私有链	联盟链
中心化程度	去中心化	中心化	部分中心化
参与者	任何用户	指定成员	联盟成员
优点	可信度高	安全性高、延迟低	可扩展性好
缺点	延迟高、效率低	节点受限、中心化	存在信任问题

即使区块链拥有去中心化、不可窜改性、高容错性及分布式一致性等良好特性，却仍然无法保证最初的产品信息是可靠的，即区块链技术并不能从源头上防止虚假产品信息输入区块链[21]，还需要结合物联网技术(如传感器、状态检测器等)来保证产品信息完整可靠客观地传输到区块链上。因此，本文基于私有链和联盟链以及物联网技术设计防伪溯源系统，在确保源头数据客观有效的前提下，保证链上产品信息真实可靠可溯源。

2　基于双链及物联网技术的防伪溯源系统设计

2.1　防伪溯源系统参与者设定

产品溯源的功能和性质决定了其拥有诸多的参与者，主要包括各个生产企业、国家相关部门以及消费者等。产品溯源系统在要求拥有一定开放性的同时，也必须包含足够的隐私性和安全性。本文提出使用联盟链和私有链的防伪溯源系统，其中联盟链主要用于产品溯源信息的查询和共享，私有链将用于收集和存储各企业产品溯源信息，再通过哈希指针与联盟链相连。采用此设计方式有利于减轻联盟链网络传输的负担，提高消费者产品数据查询的效率，同时私有链保证了企业产品数据的安全隐私，不仅数据存储效率高，还能够满足各参与方对溯源系统的需求。

各企业中的生产部门、运输仓储部门、销售部门、信息技术部门及国家监管部门等共同维护私有链，向私有链中添加产品溯源信息及监管部门的审核信息。其中，国家监管部门将作为私有链组织者的身份，对参与到私有链网络中的企业进行审核授权，信息技术部门作为私有链的记账权拥有者，负责收集信息打包区块。各企业中的其他部门及国家执法部门等共同维护联盟链，对外提供溯源信息查询功能。

2.2　产品溯源信息结构

由于区块链无法防止最初的数据造假，即无法防止非法企业伪造产品原材料、仓储等信息，所以各企业将利用物联网技术对生产、加工和仓储进行实时监控，建立一套智能化的生产线和仓储线，保证源头数据的真实可靠性。

如图 4 所示，对于某产品，企业生产部门所生成的生产信息 P 包括但不限于：产品 ID、产品名、原材料信息(由传感器记录并传输到生产部门)、负责人签名 S_x 及生产信息的哈希值 H(P)。

产品ID	产品名	原材料信息	S_x	H(P)

图 4　生产信息 P

Fig. 4　Production information

如图 5 所示，对于某产品，企业运输仓储部门产生的运输仓储信息 T 包括但不限于：运输时间、运输方式、仓储信息(通过温度传感器等传输)、负责人签名 S_Y 及运输仓储信息的哈希值 H(T)。

运输时间	运输方式	仓储信息	S_Y	H(T)

图 5　运输仓储信息 T

Fig. 5　Transportation and warehousing information

如图 6 所示，对于某产品，企业销售部门产生的销售信息 S 包括但不限于：销售时间、销售数量、销售方式、负责人签名 S_Z 及销售信息 S 的哈希值 H(S)。

销售时间	销售数量	销售方式	S_Z	H(S)

图 6　销售信息 S

Fig. 6　Sales information

为了防止企业自身窜改产品溯源信息，上述三类溯源信息还要交由国家监管部门进行审核，得到审核信息 C。利用哈希函数输入敏感的特性，检查溯源信息是否被窜改，如发生窜改，可以根据各流程中负责人的签名快速进行责任确权，以防止非法产品的流通。如没有发生窜改，则交由企业信息技术部门处理。

国家监管部门审核无误后，企业信息技术部门收集生产信息 P、运输仓储信息 T、销售信息 S、审核信息 C，结合信息技术部门负责人签名 S_i 共同构成私有链区块中的一笔交易，其结构如图 7 所示。

生产信息P	运输仓储信息T	销售信息S	审核信息C	S_i

图 7　私有链交易结构

Fig. 7　Transaction structure of private chain

重复上述过程后，将生成一条安全可靠的产品溯源信息私有链。为了防止企业隐私数据泄露，企业在私有链上只能查询本企业生产的产品信息。由于私有链中传输数据量大，不适合在提供查询功能的联盟链中传输。因此，在联盟链区块体中没有必要存储完整的产品溯源信息，而是存储私有链中每个区块的区块头哈希值即可。这样不仅能够提高数据在联盟链中传输的效率，同时根据 Merkle tree 和哈希函数的特性，产品溯源信息将一一对应，不存在溯源信息错乱的情况。联盟链中区块的区块头包括当前区块哈希值、前一个区块头的哈希值、时间戳、Merkle Root 及相关负责人签名，区块体则包含私有链中每个区块头的哈希值。图 8 为私有链和联盟链的数据结构。

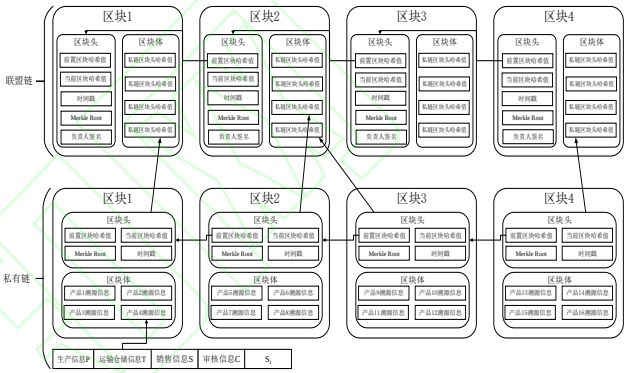

图 8　私有链和联盟链的数据结构

Fig. 8　Data structure of private chain and alliance chain

2.3　伪代码表示

定义各个部门为 D_j，$j \in 1,2,3\ldots n$，其中生产部门为 D_1，运输仓储部门为 D_2，销售部门为 D_3，信息技术部门为 D_4，国家监管部门为 D_5，国家执法部门为 D_6。原材料信息为 RD，仓储信息为 WD，负责人签名为 S_n，$n \in X,Y,Z,i$，传感器表示为 Sen。

在 2.2 节所描述的过程的伪代码表示如下：

算法 1　溯源数据生成

输入：原材料信息 RD，仓储信息 WD。

输出：生产信息 P 及其哈希值 H(P)，运输仓储信息 T 及其哈希值 H(T)，销售信息 S 及其哈希值 H(S)。

```
Begin
Sen.Generate(RD,WD)  # 传感器获取原材料信息 RD,WD
for j in Dj∈(D1,D2,D3):
Sen.trans((RD,WD), Di)  # 传输原始数据给对应部门
Dj.Generate(K) K∈P,T,S # 各部门生成对应的信息
for i in K:
Sn = Di.Sign(K) # 部门负责人对信息签名
Hi = Hi.append(K) # 信息的哈希值
send(K, Sn, Hi, D5) # 信息传输给国家监管部门审核
End
```

算法 2　溯源数据审核

输入：生产信息 P 及其哈希值 H(P)，运输仓储信息 T 及其哈希值 H(T)，销售信息 S 及其哈希值 H(S)，各信息负责人签名 S_n。

输出：审核信息 C 及其哈希值 H(C)。

```
Begin
if check(Sn):  # 验证信息的负责人签名
Then if Hi == Hash(K):  # 签名无误后，在验证哈希值
Then D5.generate(C)  # 哈希值无误后，生成审核信息 C
```

```
else:
pop(K) # 溯源数据有误
notice(Di) # 通知相关企业部门整改
End if
else:
pop(Sn)  # 签名有误
notice(Di)  # 通知相关企业部门整改
End if
D5.send(K,C,H(C),Sc,D4)  #溯源数据和审核数据传输给信息技术部门
End
```

算法 3 溯源数据存储

输入：生产信息 P，运输仓储信息 T，销售信息 S，审核信息 C。

输出：私有链新区块

```
Begin
D4.get(K, C)  # 信息技术部门获取溯源数据和审核数据
if check(H(C)) and check(Sc):
Then New_tranction.Generate(P,T,S,C) # 生成新的交易数据
H = Hash(New_traction)  # 生成数据的哈希值
Si = Sign(H) # 负责人签名
End if
# 生成新区块
D4.Generate(new_block(H, pre_H, New_tranction, Si))
Link(new_block, Private_chain)  # 新区块加入私有链
End
```

算法 4 生成联盟链

输入：私有链区块头哈希值 H(Private_chain_header)。

输出：联盟链新区块

```
Begin
D6.get(Private_chain_block) # 收集区块
H = H(Private_chain_header) # 生成数据的哈希值
Si = Sign(H) # 负责人签名
New_tranction.Generate(H) # 生成新的交易数据
if check(New_tranction):
Then D6.Generate(new_block(H, pre_H, New_tranction, Si))
# 生成新区块
link(new_block, Alliance_chain) # 新区块加入联盟链
End
```

3　溯源信息查询机制

产品溯源系统除了保证数据的真实可靠，打破信息孤岛，为企业厘清责任外，也应当为消费者提供高效精准的产品溯源信息查询功能。在本文所述的防伪溯源系统中，将由国家相关部门建立产品溯源平台，作为对外查询溯源数据的接口，联盟链和私有链将作为此平台的数据来源。如图 9 所示，在购买产品后，消费者可以登入产品溯源平台，发起对相关产品溯源的请求，溯源平台首先对该请求进行判定，若为合法的请求，则交由联盟链处理，再向私有链相关企业请求查阅相关产品的溯源信息，企业返回数据后，溯源平台将进一步匹配是否与消费者请求一致，然后再将溯源数据发送给消费者。其中，对消费者溯源请求是否合法的审核依据包括消费者的请求频率和购买记录[7]。

4　仿真实验与分析

4.1　仿真环境设置

本次仿真实验主要采用三台 PC 机，通过搭建仿真私有链、联盟链和溯源平台实现溯源。其硬件配置信息及主要承担的功能，如表 2 所示。

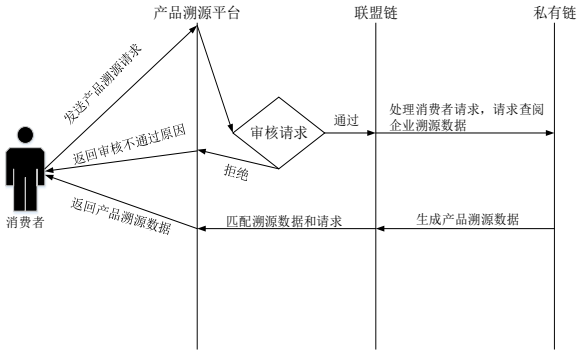

图 9　溯源信息查询机制示意图

Fig. 9　Diagram of traceability information query mechanism

表 2　实验环境说明

Tab. 2　Experiment environment description

名称	CPU/内存	操作系统	主要功能
PC1	i5-7500/4G	Ubuntu16.04	部署私有链
PC2	i5-7500/4G	Ubuntu16.04	部署联盟链
PC3	i5-7500/8G	Windows 10	搭建溯源平台

4.2　实验仿真与结果分析

根据第 2 节的设计思路，实验首先在 PC1 上搭建了简易的私有链系统，用以存储详细的产品溯源数据，其中对于原材料信息和仓储信息粗略地表示为产品产地和原料存储地。图 10 表示的是私有链区块结构和交易结构。实验模拟了二十种产品的溯源数据，根据 previous_hash 前后相连，实现可追溯的功能，同时对该数据的任何修改，都将破坏链式结构，保证数据的不可窜改性。

图 10　私有链区块结构和交易结构

Fig. 10　Private chain block and transaction structure

之后，在 PC2 上搭建了简易的联盟链系统，用以保存私有链区块头的哈希值。图 11 为联盟链区块结构和交易结构。

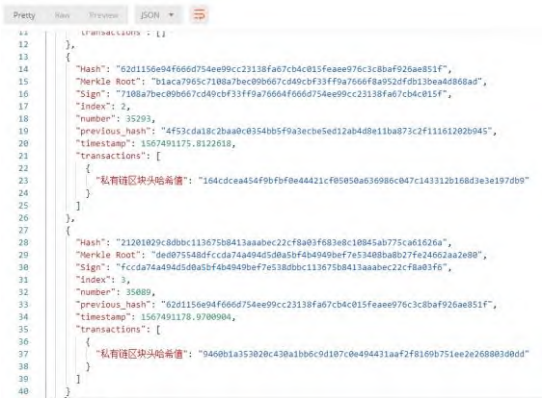

图 11　联盟链区块结构和交易结构

Fig. 11　Alliance chain block and transaction structure

最后，在 PC3 上搭建小型产品信息溯源平台，其数据来源分别来自私有链和联盟链。图 12 以及图 13 模拟的是用户针对某产品发起溯源请求的过程。对于某产品溯源数据的查询，用户输入商品名后，系统会自动取其哈希值，然后在联盟链处理过后，交由私有链相关区块进行查找，先将数据返回平台匹配请求，再返回给用户数据。如果未能找到相关溯源信息，则用户可以提交反馈。

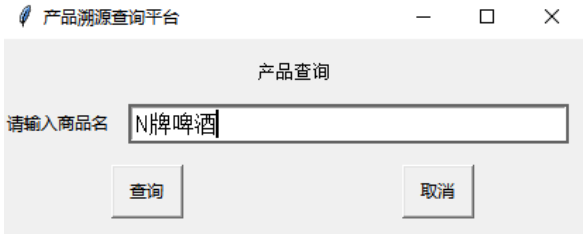

图 12　溯源数据查询

Fig. 12　Query traceability data

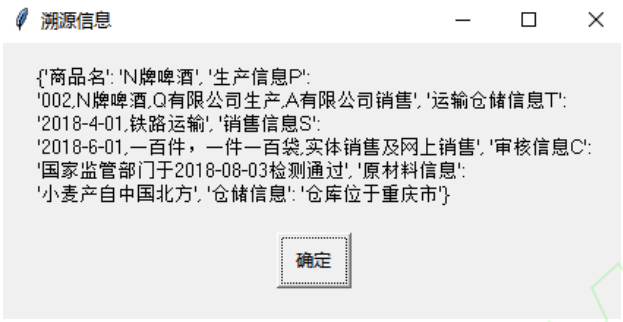

图 13　溯源数据展示

Fig. 13　Display traceability data

在系统性能方面，本文所提出的防伪溯源系统的主要时间花费在溯源数据的收集、传输和审核。在溯源数据的生成过程中，传感器能够实时传输准确数据，消耗的时间较少，而各部门生成各自信息也主要取决于网络因素。如图 14 所示，在普通的网络条件下，对本文搭建的系统进行 20 次测试，其中私有链交易数据的生成时间在 524ms 到 890ms 之间，平均值为 632ms。联盟链交易数据的生成时间在 513ms 到 773ms 之间，平均值为 617ms。而在私有链查询所有区块时间几乎和联盟链查询所有区块时间相等，均在 500ms 左右，在图中基本重合，同时用户查询溯源数据的时间在 383ms 到 493ms 之间，平均为 430ms。

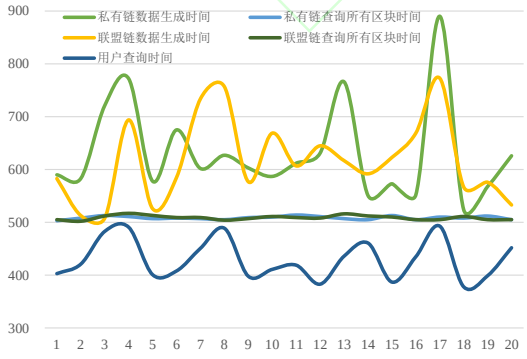

图 14　系统性能测试

Fig. 14　System performance test

4.3　系统优势与不足

在本次仿真实验中，模拟了用户对产品溯源的过程，验证了本文所论述防伪溯源系统的可行性，实现了产品溯源的功能。但是本实验仅仅使用了小样本集完成溯源功能，而在真实的生产环境中，数据将更为庞大和复杂，系统还需要进一步的完善和优化。

5　安全性分析

本文所提出的基于双区块链及物联网技术的防伪溯源系统具备较强的安全性，其安全性主要体现在以下方面：

a) 基于区块链本身具有的安全性，如去中心化、不可窜改和高容错性等。任何对产品溯源数据的修改，都将不可避免的破坏区块链链式结构，增加数据修改的成本与难度，保证溯源数据的真实可靠，同时也能在一定程度上督促企业在产品生产过程中不造假。

b) 结合物联网技术，生成真实、客观的产品数据并传输到相关部门的产品数据中，封堵数据源头造假的可能，提高产品溯源数据的安全可靠性。

c) 采用联盟链和私有链的双链结构能够保证区块链运行环境的高可信度。联盟链和私有链的建立、部署及运行本身基于一种可信的合作关系，所有的参与者再加入区块链网络之前就已经过审核，这将大大降低系统中出现恶意节点的可能，也就能够防范内部攻击，进一步提高系统的安全性。

6　结束语

在产品安全越来越受到人们关注的前提下，本文分析了传统产品溯源系统出现的诸如溯源信息不可靠、产品信息不对称，发生安全事故时责任人定位困难等难题，梳理了其他学者对产品溯源领域的相关工作，阐述了区块链的技术特点和分类以及实现信息可追溯及不可窜改的过程，提出了基于双区块链和物联网技术的防伪溯源系统，在保证产品溯源数据的安全可靠的同时，确保产品源头数据的真实客观，并通过仿真实验验证了系统的可行性，对区块链技术和产品安全领域的进一步结合提供了参考和借鉴。

目前，应用区块链技术的产品防伪溯源系统仍处于初期的摸索阶段，其适用的产品类型还需要进一步分析，与物联网技术的融合还存在着一些安全问题。下一步工作将继续细化二者结合的细节问题以及完善产品溯源系统。

此外，除了在技术上保证产品的安全，国家有关部门也应该充分发挥自身的职能作用，如加强对生产企业的监管力度、完善相关法律制度、培养公众产品安全意识等。相信在技术创新和行政管理的共同作用下，公众能够重拾对产品安全的信心。

参考文献：

[1] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system [EB/OL]. (2018-11-01) [2019-07-29]. http://www. bitcoin. org/bitcoin. pdf.

[2] 刘耀宗, 刘云恒. 基于区块链的 RFID 大数据安全溯源模型 [J]. 计算机科学, 2018, 45 (11A): 367-368, 381. (Liu Yaozong, Liu Yunheng. Security provenance model for RFID big data based on blockchain [J]. Computer Science, 2018, 45 (11A): 367-368, 381.)

[3] 张昕伟, 张华, 郭肖旺, 等. 基于区块链的电子投票选举系统研究分析 [J]. 电子技术应用, 2017, 43 (11): 132-135. (Zhang Xinwei, Zhang Hua, Guo Xiaowang, *et al.* Reasearch and analysis of electronic voting system based on blockchain [J]. Application of Electronic Technique, 2017, 43 (11): 132-135.)

[4] 佘维, 陈建森, 刘琦, 等. 一种面向医疗大数据安全共享的新型区块链技术 [J]. 小型微型计算机系统, 2019, 40 (7): 1449-1454. (She Wei, Chen Jiansen, Liu Qi, *et al.* New blockchain technology for medical big data security sharing [J]. Journal of Chinese Computer Systems, 2019, 40 (7): 1449-1454.)

[5] Elizabeth W. How blockchain can bring financial services to the poor [EB/OL]. (2017) [2019-07-29]. https://www. technologyreview. com/s/60414 4/how-blockchain-can-lift-up-the-worlds-poor/.

[6] Walport M. Distributed ledger technology: Beyond block chain [EB/OL]. (2016) [2019-07-29]. https://www.gov.uk/government/news/distributed-ledger-technology-beyond-block-chain.

[7] 丁庆洋，朱建明，张瑾，等. 基于双层架构的溯源许可链共识机制 [J]. 网络与信息安全学报，2019, 5 (2): 1-12. (Ding Qingyang, Zhu Jianming, Zhang Jin, *et al.* Traceability permissioned chain consensus mechanism based on double-layer architecture [J]. Chinese Journal of Network and Information Security, 2019, 5 (2): 1-12.)

[8] 张国英，毛燕琴. 一种基于区块链的去中心化数据溯源方法 [J]. 南京邮电大学学报：自然科学版，2019, 39 (2): 91-98. (Zhang Guoying, Mao Yanqin. Blockchain-based decentralized data provenance method [J]. Journal of Nanjing Unversity of Posts and Telecommunications: Natural Science Edition, 2019, 39 (2): 91-98.)

[9] Abeyratne S, Monfared R. Blockchain ready manufacturing supply chain using distributed ledger [J]. International Journal of Research in Engineering and Technology, 2016, 5 (9): 1-10.

[10] FENG T. An agri-food supply chain traceability system for China based on RFID & blockchain technology [C]// Proc of the 13th International Conference on Service Systems and Service Management. NJ: IEEE Press, 2016: 1-6.

[11] FENG T. A supply chain traceability system for food safety based on HACCP, blockchain & Internet of things [C]// Proc of International Conference on Service Systems and Service Management. NJ: IEEE Press, 2017: 1-6.

[12] Huertas. Eximchain: Supply Chain Finance solutions on a secured public, permissioned blockchain hybird. [EB/OL]. (2018-03-13) [2019-07-29]. https://eximch ain. com/documents.

[13] Biswas K, Muthukkumarasamy V, Lum W. Blockchain based wine supply chain traceability system [C]// Proc of Future Technologies Conference. 2017: 56-62.

[14] 刘家稷，杨挺，汪文勇. 使用双区块链的防伪溯源系统 [J]. 信息安全学报，2018, 3 (3): 17-29. (Liu Jiaji, Yang Ting, Wang Wenyong. Traceability system using public and private blockchain [J]. Journal of Cyber Security, 2018, 3 (3): 17-29.)

[15] 武岳，李军祥. 区块链共识算法演进过程 [J/OL]. 计算机应用研究，2019, 37 (7): 1-9. (2019-05-17) [2019-07-29]. http://www. arocmag. com/artic le/02-2020-07-004. html. (Wu Yue, Li Junxiang. Evolution process of blockchain consensus algorithm [J/OL]. Application Research of Computers, 2019, 37 (7): 1-9. (2019-05-17) [2019-07-29]. http://www. arocmag. com/article/02-2020-07-004. html.)

[16] 工业和信息化部. 中国区块链技术和应用发展白皮书 [EB/OL]. (2016-10-18) [2019-07-29]. https://www. jianshu. com/p/6ac84516a4c5. (Ministry of Industry and Information Technology. China blockchain technology and application development white paper [EB/OL]. (2016-10-18) [2019-07-29]. https://www. jianshu. com/p/6ac84516a4c5.)

[17] Szydlo M. Merkle tree traversal in log space and time [C]// Proc of International Conference on the Theory and Applications of Cryptographic Techniques, 2004: 541-554.

[18] R. L. Trope and E. K. Ressler. Mettle Fatigue: VW's Single-Point-of-Failure Ethics [J]. IEEE Security & Privacy, 2016, 14 (1): 12-30.

[19] Buterin V. On public and private blockchains [EB/OL]. (2015-08-06) [2019-07-29]. https://blog. ethereum. org/2015/08/07/on-public-and-private-blockchains.

[20] 袁勇，倪晓春，曾帅，等. 区块链共识算法的发展现状与展望 [J]. 自动化学报，2018, 44 (11): 2011-2022. (Yuan Yong, Ni Xiaochun, Zeng Shuai, *et al.* Blockchain consensus algorithms: The state of the art and future trends [J]. Acta Automatica Sinica, 2018, 44 (11): 2011-2022.)

[21] 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. (Ding Qingyang, Zhu Jianming. The product information traceability and security model of B2C E-platform from the perspective of blockchain [J]. China Business and Market, 2017, 31 (12): 41-49.)