面向冷链物流的区块链技术方案研究与实现

张 森[1,2],叶 剑[2],李国刚[1]
1.华侨大学 信息科学与工程学院,福建 厦门 361021
2.中国科学院 计算技术研究所,北京 100190

摘 要:目前的冷链物流系统大都采用中心化的解决方案,数据管理由物流企业独自完成,出现了一系列信任问题。针对这些问题,提出了一种面向冷链物流行业的区块链技术解决方案,利用区块链特有的去中心化、去信任化的特点,针对订单数据和环境数据分别设计上链系统,实现了订单数据安全上链、冷链环境数据实时上链以及物联网设备的身份认证与权限控制机制,提高了冷链物流行业的可信性和数据的安全性。通过系统原型实现与测试,表明该方案可以满足业务需求,对冷链物流行业有重要影响。

关键词:冷链物流;区块链; Fabric;智能合约; 物联网
文献标志码:A **中图分类号:**TP311 doi:10.3778/j.issn.1002-8331.1908-0453

张森,叶剑,李国刚.面向冷链物流的区块链技术方案研究与实现.计算机工程与应用,2020,56(3):19-27.
ZHANG Sen, YE Jian, LI Guogang. Research and implementation of blockchain technology scheme for cold chain logistics. Computer Engineering and Applications, 2020, 56(3):19-27.

Research and Implementation of Blockchain Technology Scheme for Cold Chain Logistics

ZHANG Sen[1,2], YE Jian[2], LI Guogang[1]
1.College of Information Science and Engineering, Huaqiao University, Xiamen, Fujian 361021, China
2.Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100190, China

Abstract: Most of the current cold chain logistics systems use centralized solutions. Data management is done by logistics companies alone, and a series of trust problems have emerged. Aiming at these problems, a blockchain technology solution for the cold chain logistics industry is proposed. By using the characteristics of decentralization and de-trusting unique to the blockchain, a chain-up system is designed for the order data and environmental data. The order data security chain, cold chain environment data real-time uplink and IoT device identity authentication and authority control mechanism improve the credibility and data security of the cold chain logistics industry. Through the system prototype, it shows that the program can meet the business needs and has an important impact on the cold chain logistics industry.

Key words: cold chain logistics; blockchain; Fabric; smart contract; Internet of Things(IoT)

1 引言

近年来,随着人们生活水平的不断提高以及电子商务的普及,我国冷链物流市场也快速发展。所谓冷链物流,泛指一些特殊商品(比如食品、药品)在其加工、贮藏、运输、分销、零售等各环节,需要始终保持一定温度的物流运输方式,从而保证商品质量[1]。

目前的冷链物流系统大都采用物联网技术来提高物流系统的信息化水平,比如文献[2]通过物联网技术实现对冷链中货物的有效、快速的监控,但这种方式没有解决数据中心化存储的弊端,仍然存在以下问题[3-4]:(1)缺乏信任的问题。冷链物流行业要求高,成本高,数据造假、跑路等不信任行为频频出现,大大提高了货损

基金项目:国家重点研发计划(No.2017YFB1302400);2018年工信部工业互联网创新发展项目;2019年工业互联网创新发展工程项目;华侨大学研究生科研创新基金(No.17014082028)。
作者简介:张森(1992—),男,硕士研究生,研究领域为区块链应用,物联网技术,E-mail:1186309973@qq.com;叶剑(1974—),男,博士,高级工程师,CCF会员,研究领域为普适计算,嵌入式系统,区块链;李国刚(1973—),男,博士,副教授,研究领域为密码学,物联网技术,区块链。
收稿日期:2019-08-30 **修回日期:**2019-10-28 **文章编号:**1002-8331(2020)03-0019-09
CNKI **网络出版:**2019-11-13, http://kns.cnki.net/kcms/detail/11.2127.TP.20191113.1508.012.html

率。(2)运输过程不透明。物流企业在运输过程中,为了降低成本,可能存在运输过程中关闭制冷机、快到目的地时再打开制冷机的现象,不能做到全程冷链。(3)数据存储不透明。现在温度数据大多存储在承运方和仓储企业的中心化数据库中,货主无法方便获取数据。中心数据库记录的方式可靠性不高,重要数据需要进行冗余备份。(4)资源共享难度大。在采用第三方物流运输时,尤其在农产品领域,存在货物分散的特点。目前存在着运力不透明的问题,难以实现资源共享和设备利用的最大化。

为此,本文提出一种面向冷链物流行业的区块链技术解决方案,利用区块链技术所具有的去中心化、去信任化、数据防篡改等特点[5],建立安全可信的冷链物流数据共享机制,提高运输过程、数据存储等环节的透明性。

2 相关工作

2.1 区块链

随着比特币等电子货币的广泛传播,作为其底层核心模块的区块链技术成为工业界和学术界讨论的热点[6]。所谓区块链技术是一种由多方共同维护的,使用密码学保证传输和访问安全,能够实现一致性存储、难以篡改、防止抵赖的记账技术,也称为分布式账本技术[7]。到目前为止区块链技术已经经历了三个发展阶段[8-10],即数字货币为代表的区块链1.0时代;融入智能合约的区块链2.0时代;将区块链应用于更多行业场景的区块链3.0阶段。在区块链系统中,所有已提交的事物都存储在链中,当新的交易被确认时,将增加链的长度,而不会对前面的数据进行修改,从而保证了数据的完成性[11]。区块链系统具有分布式高冗余存储、时序数据且不可篡改和伪造、去中心化信用、自动执行的智能合约、安全和隐私保护等显著的特点[12],使得区块链的应用已从金融领域延伸到实体领域,电子信息存证、版权管理和交易、产品溯源、数字资产交易、物联网、智能制造、供应链管理等领域[13]。例如,薛腾飞等人[14]提出一个基于区块链的医疗数据共享模型,适用于解决各医疗机构数据共享的难题;瑞士初创公司Modum[15]与苏黎世大学合作设计了一套基于区块链的制药供应链系统,以确保药物的安全运送;Guan等人[16]研究了区块链技术在智能电网中的应用;Elisa等人[17]提出了一种基于区块链技术的电子政务系统,增进了各公共部门之间的信任;Cobe等人[18]设计了一种应用于联网车辆信息管理的区块链框架。

根据实际应用场景和需求,区块链技术可以分为三种应用模式,即公共链、联盟链和私有链[19]。公共链是以比特币为代表的最初的区块链形态,任何节点都可以自由加入,并参与到账本数据的读写、验证和共识,共同维护账本数据;联盟链是一种有准入控制机制的区块链形态,适用于多个实体构成的组织或者联盟;私有链是一种中心化的区块链形态,完全由一个组织控制,适用于特定机构的内部数据管理和审计。

2.2 Hyperledger Fabric

Hyperledger Fabric[20]是一种被广泛应用的联盟区块链平台,以模块化架构为基础,提供可切换、可扩展的组件,具有高度的保密性、弹性、可扩展性和灵活性。其克服了比特币、以太坊等公有链项目吞吐量低、无隐私机制、共识算法低效等的缺陷,更适用于商业场景,使用户能够方便地开发商业应用。

在Fabric网络模型中,主要包括客户端节点、Peer节点、CA节点和Orderer节点四种组件。客户端节点主要作用是和Fabric系统交互,实现对区块链系统的操作,包括管理类操作和链码类操作。Peer节点是区块链去中心化网络中的对等节点,按照功能主要划分为背书节点(Endorser)和确认节点(Committer)。背书节点主要对交易预案进行校验、模拟执行和背书签名,确认节点则负责检验交易的合法性,并更新和维护区块链数据和账本状态。Orderer节点是排序服务节点,负责对各个节点发过来的交易进行排序。CA节点主要是给Fabric网络中的成员提供基于数字证书的身份信息,可以生成或者注销成员的身份证书。

2.3 Diffie-Hellman密钥交换算法

Diffie-Hellman[21](简称DH)是密钥交换算法之一,它的作用是保证通信双方在非安全的信道中安全地交换密钥。在DH算法中,发送方和接收方共同产生一个只有双方知道的私有的密钥,其产生过程是使用自己的私钥和对方的公钥经过计算得到共享密钥。

首先,通信双方A和B协商一个大的素数 n 和 g ,g 是模 n 的本原元,这两个数不必是秘密的。故A和B可以通过不安全的途径协商它们,它们也可以在一组用户中公用。其主要运算过程如下:

(1)A选取一个大的随机整数 x ,并计算 $X=g^x \bmod n$,将 X 发送给B。

(2)B也选取一个大的随机整数 y ,并计算 $Y=g^y \bmod n$,将 Y 发送给A。

(3)A计算 $k=Y^x \bmod n$ 。

(4)B计算 $k'=X^y \bmod n$ 。

经过以上过程,则有 $k=k'=g^{xy} \bmod n$,因此,k 和 k' 可以看做是通信双方各自独立计算,又相互知道的密钥。

3 方案整体设计

3.1 整体架构

本文提出的面向冷链物流行业的区块链技术解决

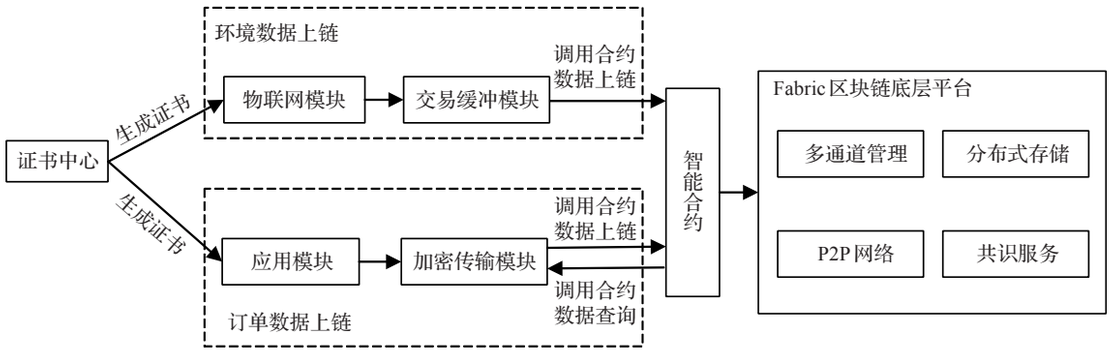

图1　方案整体架构示意图

方案,主要利用物联网技术和区块链技术相结合,其整体架构如图1所示,包括证书中心机构、环境数据上链模块、订单数据上链模块、智能合约模块以及Fabric区块链底层平台[22]。

(1)证书中心机构负责为物联网设备和区块链网络模型中各组织的Peer节点、Orderer节点、用户等提供数字证书的生成、身份的认证。(2)环境数据上链模块包括物联网模块和交易缓冲模块。物联网模块主要负责冷链过程的环境数据的采集与处理。交易缓冲模块通过引入消息队列机制对物联网模块传输来的数据进行缓存。(3)订单数据上链模块包括应用模块和加密传输模块。应用模块通过调用证书中心的相关接口实现各组织用户的注册、证书的生成,以及通过调用智能合约中的程序实现订单数据的上链和查询操作。加密传输模块对每一笔订单数据信息加密后上传到区块链网络,保证订单信息不会被非相关方获取。(4)智能合约模块负责提供数据上链和查询的接口,包括合约的部署、初始化、实例化、链码交互。冷链物流的各参与主体部署相同的智能合约,一旦合约容器建立,合约内容将无法修改。(5)Fabric区块链底层平台是整个系统的核心组成部分,主要有四个方面的功能,一是通过多通道隔离机制,为每个物流过程创建一个自己独有的通道实现数据隔离和商业信息保护;二是使用分布式账本存储技术实现账本数据、区块索引、状态数据、历史数据等存储结构;三是基于Gossip的P2P数据分发,Gossip模块负责连接排序服务和Peer节点,实现从单个源节点到所有节点高效的数据分发,实现不同节点的状态同步、动态节点的增加和网络分区;四是基于Kafka的排序服务,利用Kafka作为交易的消息队列,实现共识服务,保证各节点数据的一致性。

3.2　网络结构

冷链物流主要涉及发货方、物流企业、收货方等多种业务角色,三方作为冷链物流中的上下游企业都是利益相关方,每笔业务由三方共同完成,且需要实现可信的数据共享、冷链数据的可追溯防篡改。因为物流平台中会包含其他的发货方或者收货方,所以为保护商业机密并实现数据隔离,系统将引入Fabric的多链多通道机制,为每个物流过程创建一个通道,每个通道内只包含此次物流过程涉及的组织[23]。在单个通道内,本方案的网络结构模型,如图2所示。

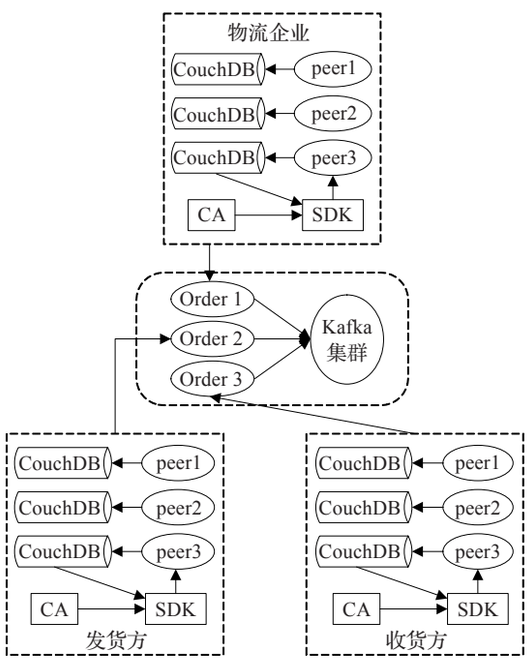

图2　冷链物流系统网络模型图

发货方、物流运输方、收货方三方映射为Fabric中的三个组织,三个组织处于相互对等的地位,形成联盟式管理方式,三方共同参与联盟链的管理。该系统选择基于Kafka的共识机制,实现高吞吐量的数据分发。每个组织内有一个CA服务器,用来生成组织内的相关证书(包括组织的证书、组织中所有节点的证书,组织中所有用户的证书),只有获得证书的用户,才能通过调用SDK的相关接口对区块链数据进行操作。每个组织内可以包含多个Peer节点,每个Peer节点都将部署相关链码,分别承担数据背书、数据备份以及通信等任务。同时本方案还将给每个Peer节点配置了CouchDB数据库,以实现更为丰富的查询功能。

4　身份认证

身份认证是区块链网络建立和数据上链的基础,只有经过认证的节点才能加入区块链网络、只有经过认证的用户才能执行数据上链和查询。本方案基于Fabric的认证体系,实现节点的身份认证、物联网设备的身份认证。

4.1　节点的身份认证

节点的身份认证主要包括Orderer节点和Peer节点的身份注册并生成MSP证书。所谓MSP即成员管理服务,用户抽象化各成员间的控制结构关系。首先,根据所设计的网络模型修改配置文件信息,即每个组织对应一个MSP,一个组织内包含三个Peer节点,一个排序服务节点,一个CA节点。然后,cryptogen模块会根据配置文件生成后续模块运行所需要的MSP证书文件,每个MSP证书文件中包括根CA证书、中间CA证书和管理员证书等。接下来,需要将生成的证书信息配置到创世区块和创世交易中,生成创世区块和创世交易通道文件。至此,节点的身份认证与通道配置完成,只需要等待区块链网络启动即可。

4.2　物联网设备的身份认证

物联网设备的身份认证采用将设备MAC地址写入到数字证书中的方法,使得物联网设备和数字证书一一对应,避免盗用数字证书使用其他设备上传虚假数据的行为。具体流程如图3所示。

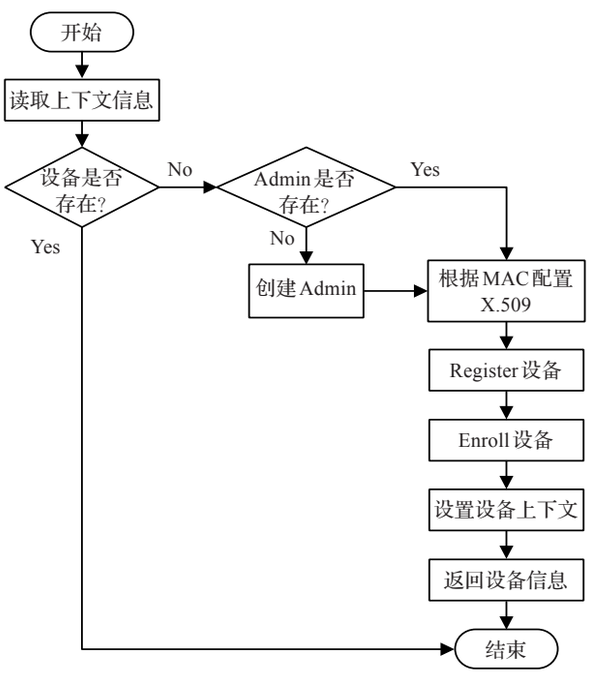

图3　物联网设备身份认证流程图

步骤1　服务器端根据设备ID读取上下文信息。

步骤2　根据读取到的配置信息判断该设备是否存在,如果设备已经存在,则返回设备信息,如果设备不存在,则进入步骤3。

步骤3　获取负责提交设备注册信息的Admin信息。

步骤4　判断登记员Admin是否存在,如果存在,则进入步骤6,如果不存在,则进入步骤5。

步骤5　初始化登记员Admin信息,配置Admin的hf.Registrar.Roles属性,使其获得登记员的登记权限,然后再配置Attributes属性,使其具有登记物联网设备的权限,然后再通过fabric-ca服务器创建Admin实例。

步骤6　根据物联网设备的MAC地址,配置其X.509证书参数,设置设备ID,设置设备所属公司部门,设置设备的唯一标识符MAC地址,设置证书角色为user。

步骤7　登记员向fabric-ca服务器调用register请求,登记设备信息,fabric-ca服务器验证请求生成用户注册的Secret。

步骤8　利用设备信息和返回的Secret,调用Enroll接口,请求生成证书和私钥。

步骤9　保存设备信息,并设置设备的Context。

经过以上步骤,每个物联网设备都有一个唯一的身份证书,且身份证书和自己的物理信息相关联,以后每次请求区块链网络将会验证设备的真实性,从而保证了数据来源的真实性。

5　数据上链系统

本方案中数据主要分为两类:订单数据和环境数据。其中,订单数据指物流订单信息,包括收发人地址、联系方式、商品信息等,该数据包含大量公民个人信息,为防止公民个人信息泄露,订单数据需要经过加密传输单元上传到区块链服务器端。环境数据主要指有物联网模块的传感器设备采集是温湿度、大气压等冷链过程中的数据,考虑该数据实时性较强、且采集速度和上链速度需要实时匹配等问题,该数据需要经过消息队列模块之后进行上链。

5.1　订单数据上链系统

本系统设计的加密传输模块采用密钥交换协议(Diffie-Hellman密钥交换算法)和对称加密算法(AES对称加密算法)相结合的方案,即通过密钥交换协议产生对称加密的密钥,然后使用对称加密算法对订单信息加密,从而保证传输过程中无明文出现,保护了用户隐私,算法时序图如图4所示。

步骤1　发货方在用户客户端向区块链服务器端发送生成服务器端的公私钥的请求。

步骤2　服务器端执行DH算法的generateKeys()方法,根据设定的素数以及素数长度,产生服务器端的公私钥对。

步骤3　区块链服务器端将生成的密钥返回给用户客户端。

步骤4　创建客户端的DH实例,采用与服务器端相

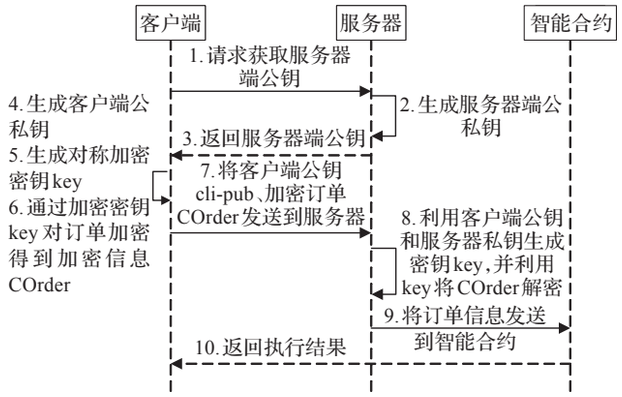

图4　加密传输模块时序图

同的素数。

步骤5　用户客户端执行DH算法的generateKeys()方法，根据设定的素数以及素数长度，产生客户端的公私钥对。

步骤6　客户端根据服务器端的公钥，计算生成对称密钥key1，并利用key1对订单信息order进行加密，生成加密后的订单信息COrder即：

Key1=client.computeSecret(serverPub)

COrder=Enc(order,key1)

步骤7　将客户端公钥cli-pub、加密订单COrder发送到区块链服务器。

步骤8　区块链服务器端根据客户端的公钥，计算生成对称密钥key2，根据DH算法可得key1恒等于key2，所以便可以利用key2将COrder解密，得到订单的详细信息，即：

Key2=server.computeSecret(clientPub)

COrderTxt=Dec(COrder,key2)

步骤9　将订单信息发送到智能合约模块，完成数据上链。

步骤10　将执行结果返回给用户客户端。

5.2　环境数据上链系统

环境数据上链系统主要包括物联网模块和消息队列模块，实现冷链环境数据的采集、处理、缓存、上链等过程。其中，物联网模块由传感器设备和Redis[24]内存数据库组成。Redis数据库为内存数据库，其读写速度非常高，能满足系统需求，Redis数据库的引入使得数据采集和数据上传分离，有效解决因上传等待延迟造成数据采集遗漏的问题，同时也起到了数据缓存和备份的作用。具体流程如图5所示。

步骤1　传感器设备负责采集温度、湿度和大气压强数据，每秒钟采集60次数据记为 $originalData$ ，将这60个数据为一组，求其平均值获得 $chainData$ ，作为最终上链的数据，以此来减小传感器采集数据的误差，即

$$originalData=[T_i,P_i,H_i]$$

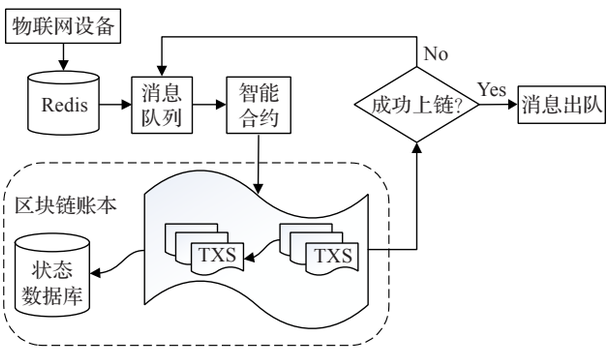

图5　环境数据上链流程图

$$chainData=\left[\frac{\sum_{i=1}^{60}T_i}{60},\frac{\sum_{i=1}^{60}P_i}{60},\frac{\sum_{i=1}^{60}H_i}{60}\right]$$

步骤2　将处理后的数据data存储在本地数据库Redis中。

步骤3　读取Redis数据库，将数据提交到区块链服务器端的交易消息队列中，返回数据提交结果。

步骤4　读取消息队列中的数据，然后提交数据到智能合约模块。

步骤5　智能合约调用相关接口将数据保存在区块链账本中，如果数据成功写入区块链账本，则相应的消息出队，如果数据写入失败，则相应的数据消息仍然保存在队列中，等待下一次上链。

6　智能合约

Fabric中的智能合约被称为链码[25]，是运行在基于Docker的安全容器中的独立应用程序，实现冷链环境数据和物流订单数据的上链(包括订单的发布、确认和签收)、状态数据查询、历史数据查询以及合约方法级的权限控制等功能。

6.1　权限控制合约

目前，Fabric不能对合约方法进行权限控制，区块链网络中的所有合法用户均可对通道内的所有合约方法进行操作，为保证环境数据上链方法只能由相应的物联网设备调用，订单数据的上链方法由组织内某一方用户调用，本方案采用与身份认证相结合的方法实现权限控制机制。首先获取调用者的证书信息，然后根据所调用的上链方法分类判断。如果调用的是环境数据上链方法，验证执行此方法的用户是否为物联网设备，其次验证该物联网设备的MAC地址和证书中的MAC地址是否一致，如果全部验证都过，则返回成功；如果调用的是发布订单方法，判断调用者是否为发货商，如果验证通过，则返回成功；如果调用的是确认订单方法，判断调用者是否为物流企业，如果验证通过，则返回成功；如果调用的是签收订单方法，判断调用者是否为收货商，如果验证通过，则返回成功；如果不是以上情况之一，则返

回失败。权限控制合约的算法流程如下所示：

算法1 权限控制算法

输入：要执行的方法名称(function)，合约调用者的MAC地址(mac)。

输出：如果权限验证通过，则执行具体的合约方法，否则结束访问。

```
1. 获取合约调用者的证书信息
2. 解析证书信息得到组织名称certOrg，证书中的MAC地址certMac
3. IF function=="setEnvironmentData" THEN
4.    IF certOrg=="sensor" && certMAC==mac THEN
5. 执行setEnvironmentData()方法
6. ELSE
7.       break;
8.    END IF
9. ELSE IF function=="issueOrder"且certOrg=="supply" THEN
10. 执行issueOrder()方法；
11. ELSE
12.       break;
13.    END IF;
14. ELSE IF function=="confirmOrder"且certOrg=="supply" THEN
15. 执行confirmOrder()方法；
16. ELSE
17.       break;
18.    END IF;
19. ELSE IF function=="signOrder"且certOrg=="supply" THEN
20. 执行signOrder()方法；
21.    ELSE
22.       break;
23.    END IF
24. END IF
```

6.2　订单数据上链合约

订单信息包括物流订单号、发货方姓名、发货方地址、发货方电话、收货方姓名、收货方地址、收货方电话、货物信息、物流公司确认信息、收货方签收信息、订单状态，其中货物信息包括所运货物的种类以及运输所需的温湿度范围等数据，数据结构定义，如表1所示。在数据存储时，采用CouchDB作为状态数据库，将第一个字段即orderID作为key，其余各字段JSON序列化后作为value。

物流订单在创建之后，将经历不同的状态变化，其状态标识由state字段表示，状态转移过程如图6所示。

首先，发货方将confirmID和signID字段置空，state字段标为NewPublish，其余各字段按照实际信息填写完整，通过调用发布订单合约方法将物流订单信息发布到系统中，此时，订单进入新发布状态NewPublish。发布

表1　订单数据结构

字段	解释
orderID	物流订单号
sender	发货方姓名
senderAddress	发货方地址
sendPhone	发货方电话
receiver	收货方姓名
receAddress	收货方地址
recePhone	收货方电话
info	货物信息
confirmID	物流公司确认信息
signID	收货方签收信息
state	订单状态

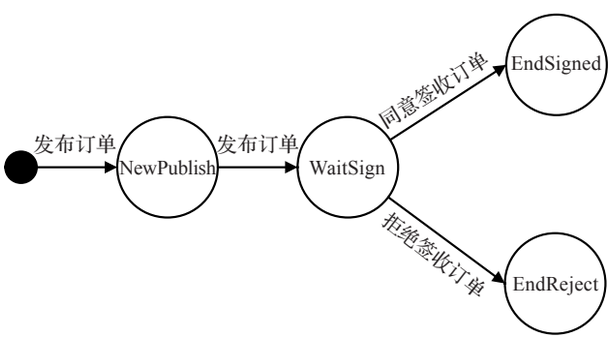

图6　物流订单状态转移图

订单的流程如下所示。

算法2 发布订单流程

输入：由物流订单号(orderID)，发货方姓名(sender)，发货方地址(senderAddress)，发货方电话(sendPhone)，收货方姓名(receiver)，收货方地址(receAddress)，收货方电话(recePhone)，货物信息(info)信息组成的json字符串args。

输出：如果订单发布成功，返回成功标识；如果订单发布不成功，返回错误信息。

```
1.  将json字符串解析成订单结构体order；
2.  orderAsBytes←GetState(order.OrderID)；
3.  IF orderAsBytes不为空THEN
4.  订单已经存在，不能发起订单；
5.  ELSE
6.       err ← PutState(order.OrderID,[]byte(args))；
7.       IF err!=nil THEN
8.  订单提交错误，返回错误信息；
9.       ELSE
10. 订单提交成功；
11.      END IF
12. END IF
```

然后，物流公司在接收到发货方的请求后，调用查询订单状态方法查看订单信息，如果确认接受此项订单，则通过调用确认订单方法填写confirmID字段信息，并将state字段标为waitSign，此时进入物流运输过程，订单处于等待签收状态waitSign。其中，确认订单的流

程如下:

算法3 确认订单流程

输入:物流订单号(orderID),物流公司确认信息(confirmID)。

输出:如果订单确认成功,返回成功标识;如果订单确认不成功,返回错误信息。

```
1.  orderAsBytes←GetState(OrderID);
2.  IF orderAsBytes==nil THEN
3.  订单不存在,不能确认订单;
4.  ELSE
5.  将订单字节信息解析成结构体order
6.      order.confirmID←confirmID
7.      order.state←waitSign
8.      err←PutState(orderID,Marshal(order))
9.      IF  err!=nil  THEN
10. 订单提交错误,返回错误信息;
11.     ELSE
12. 订单提交成功;
13.     END IF
14. END IF
```

最后,收货方查看货物后,可以通过调用签收订单方法选择签收订单和拒绝签收,如果签收订单,则填写signID字段信息,并将state字段标记为EndSigned,订单进入EndSigned状态;如果拒绝签收订单,则直接将state字段标记为EndReject,订单进入EndReject状态。签收订单的过程如下所示:

算法4 签收订单流程

输入:物流订单号(orderID),收货方签收信息(confirmID)。

输出:如果订单签收成功,返回成功标识;如果订单签收不成功,返回错误信息。

```
1.  orderAsBytes←GetState(OrderID);
2.  IF orderAsBytes==nil THEN
3.  订单不存在,不能签收订单;
4.  ELSE
5.  将订单字节信息解析成结构体order
6.      IF 签收订单 THEN
7.          order.confirmID←confirmID
8.          order.state←EndSigned
9.        ELSE IF 拒绝签收订单 THEN
10. order.confirmID←confirmID
11.         order.state←EndReject
12.     END
13.      err     ←PutState(orderID,Marshal(order))
14.     IF err!=nil THEN
15. 订单签收错误,返回错误信息;
16.     ELSE
17. 订单签收成功;
18.     END IF
19. END IF
```

6.3 环境数据上链合约

环境数据的结构如表2所示,物联网设备执行环境数据上链合约后,发货方、收货方、物流公司均可通过查询链上数据实时查看环境数据信息,通过调用查看历史数据的方法查看环境数据的历史信息。

表2　环境信息数据结构

字段	解释
iotID	物联网设备ID
temperature	采集的温度
humidity	采集的湿度
pressure	采集的大气压强
acquisitionTime	采集的时间

7 方案测试

7.1 功能测试

本方案构建了面向冷链物流的区块链网络模型,整个系统已经在测试网中运行。整个区块链网络由七台服务器构成,其中四台用于搭建Kafka集群,其余三台作为三个组织的后台服务器,每台服务器和区块链系统的配置如表3所示。

表3　测试环境配置信息

字段	值
CPU型号	Intel® Xeon® CPU E5-2620
内存	4 GB
磁盘存储	100 GB
操作系统	CentOS 7.6
Fabric版本	V1.1
Fabric SDK 版本	Nodejs sdk
树莓派	3 B
传感器	BME280环境传感器

订单数据上链与查询的测试结果如图7所示。其中图7(a)表示发货方发布订单执行后的结果以及通过订单查询可以看到订单的状态信息;图7(b)表示物流企业确认订单的执行结果以后此时订单信息;图7(c)显示了收货方签收物订单的执行结果和查询的订单信息。

环境数据上链与查询的测试结果如图8所示。

7.2 性能测试

本次性能测试主要研究每秒交易数量(TPS)的变化,测试时的主要固定参数如表4所示,图9是通过改变并发数观察每秒交易数量的变化,横轴是单次并发数,纵轴是每秒交易数,测出的每秒交易数量最高是323。如图10所示,用这种方法,经过多次测试后,系统的每秒交易数量平均值为320,该性能可以满足基本的业务需要。

通过测试分析可知,本系统通过了功能测试和性能

{"retCode":"00","retMsg":"Successfully invocked the chaincode 0rg1 to the channel 'mychannel' for transaction ID
: 9e6676c5f70fce38e7e586b589bd54afdd4e96e012987b61beaf34e030681eec","blockNumber":"2"}
{"ConfirmID":"","Info" :"Cold fresh, meat Keep the temperature between 0 and 3 degrees!","OrderID":"0000000001",
"ReceAddress":"ShangHai", "RecePhone": "18888166666","Receiver" :"LiSi","SendPhone":"18888177777","SenderAddress
":"BeiJing","SenderName":" zhangsan","SignID":" ", "State": "NewPublish"}

(a)发货方发布订单执行结果

{ "retCode":"00","retMsg":"Successfully : invoked the :chaincode 0rg2 to the channel 'mychannel' for transaction
ID: 75b5315156c8f3ef1274642397c85f4528e2e71f61d1e5e3ff10b58c95b542a4", "blockNumber" :"3"}
{ "ConfirmID":"Logistics company :001","Info":"Cold fresh meat Keep the temperature between 0 and 3 degrees!" ,
"OrderID":"0000000001","ReceAddress" : "ShangHai","RecePhone":"18888166666","Receiver":"LiSi","SendPhone":"18888
177777","SenderAddress":"BeiJing","SenderName" :"zhangsan","SignID" :" ","State":"waitSign"}

(b)物流企业确认订单执行结果

{"retCode":"00","retMsg" :"Successfully invoked:the chaincode 0rg3 to the channel'mychannel': for transaction ID
: 09d64f664ee00d5c9b1eefea4cd5c016b4dbbfc53e6d3e92390828078a8774d8", "blockNumber": "4" }
{"ConfirmID":"Logistics company 001", "Info":"Cold fresh meat Keep the temperature between 0 and 3 degrees!" ,"
OrderID":"0000000001","ReceAddress":"ShangHai","RecePhone" :"18888166666","Receiver":"LiSi","SendPhone" :"188881
77777","SenderAddress":"BeiJing", "SenderName":"zhangsan", "SignID":"LiSi001", "State" :"Endsigned" }

(c)收货方签收物订单执行结果

图7　订单数据上链结果示意图

{"retCode": "00","retMsg": "Successfully invoked the chaincode 0rg2 to the channel 'm
ychannel' for transaction ID: e1bc0028d39bd3f432875899d52484747d37c5e2e601f7df354cfba
30f420f29","blockNumber": "4"}
{"acquisitionTime":"2019-05-14--17:53:53","humidity": "26.75%","pressure":"998.35hPa"
,"sensorID":"sensor001","temperature":"28.10*C"}

图8　环境数据上链结果示意图

表4　测试环境配置信息

字段	值
总请求数	10 000
每个区块包含的最大交易数	200
区块打包最大时间间隔/s	2
组织数	3

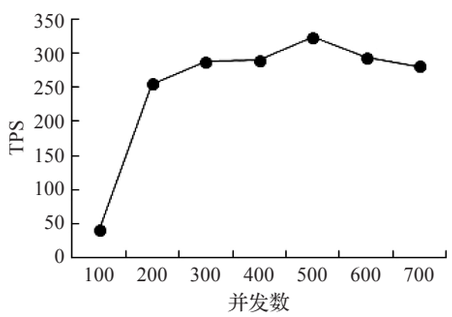

图9　TPS与并发数关系图

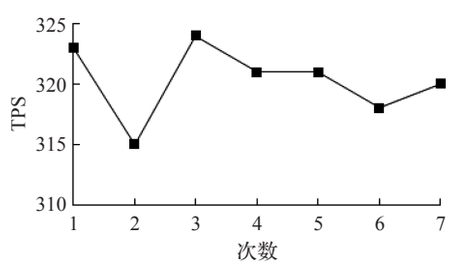

图10　多次测试结果示意图

测试,完成了预期设计目标,验证了系统的可行性和有效性。本方案的优势主要体现在,和传统中心化的冷链系统相比,构建了以区块链为底层的分布式存储方案。利用区块链技术的历史数据不可篡改,很好地增进了各企业间的互信,摆脱了一家核心企业独自掌握数据权限的情况。

8　结束语

本文将区块链技术同物联网技术相结合,提出了一种面向冷链物流行业的区块链技术解决方案,通过引入消息队列中间件,实现了异步调用合约,提高了数据上链的效率。同时,系统还会监听数据上链是否成功,由于超时等原因没有上链的数据,将会进行二次上链,从而保证消息队列里的数据都能完整的上链,即保证了数据的完整性,不会造成数据丢失。通过设计成员管理服务,保证了数据交易的安全性,即只有持有特定证书机构签发的数字证书的节点才能加入区块链网络。同时通过多通道机制,实现了数据隔离,保证只在每一次物流运输过程的相关参与方之间共享数据。通过密钥交换协议和对称加密算法相结合的方案,订单数据在传输过程中都进行了加密处理,保证了物流订单传输的安全。通过将数字证书和物联网设备的物理信息相关联,保证只有相关的物联网设备才能上传数据。总之,区块链技术和冷链物流领域的结合,必将会提高物流行业的互信,降低成本,提高安全性。

在2018年5月份,由普华永道和VeChain联合发布的《2018年中国区块链(非金融)应用市场调查报告》中显示,物流行业被业内人士认为是除金融行业之外创新应用价值最高的行业。冷链物流行业正在积极借鉴区块链技术,助推其产业升级。比如,2018年5月,由京东物流主导,国内首个“物流+区块链技术应用联盟”成立,将区块链与人工智能、物联网相结合。本文是将区块链技术应用于冷链物流领域的初步探索,下一步将会同相关企业继续完善该领域的应用,提高系统性能,提供更多服务,进一步发掘区块链在物流行业中的应用价值。

参考文献：

[1] 毋庆刚.我国冷链物流发展现状与对策研究[J].中国流通经济，2011，25(2)：24-28.

[2] Luo H，Zhu M，Ye S，et al.An intelligent tracking system based on internet of things for the cold chain[J].Internet Research，2016，26(2)：435-445.

[3] 罗建辉.拥抱区块链构建物流共信共配服务体系[J].中国物流与采购，2018(14)：53.

[4] 李刚.RFID技术在铁路冷链物流领域的应用方案[J].物流技术与应用，2017(2)：104-106.

[5] 谢辉，王健.区块链技术及其应用研究[J].信息网络安全，2016(9)：192-195.

[6] 沈鑫，裴庆祺，刘雪峰.区块链技术综述[J].网络与信息安全学报，2016，2(11)：11-20.

[7] 中国信通院.区块链白皮书[EB/OL].(2018-09-05)[2019-05-21].http://www.caict.ac.cn/kxyj/qwfb/bps/201809/t20180905_184515.htm.

[8] Barber S，Boyen X，Shi E，et al.Bitter to better—how to make bitcoin a better currency[C]//International Conference on Financial Cryptography and Data Security.Berlin，Heidelberg：Springer，2012：399-414.

[9] Wood G.Ethereum：asecure decentralised generalised transaction ledger[R].Ethereum Project Yellow Paper，2014.

[10] Pieroni A，Scarpato N，Di Nunzio L，et al.Smarter city：smart energy grid based on blockchain technology[J].International Journal on Advanced Science，Engineering and Information Technology，2018，8(1)：298-306.

[11] Ethereum.Ethereum homestead documentation[EB/OL].[2019-05-21].http://ethdocs.org/en/latest/.

[12] 袁勇，王飞跃.区块链技术发展现状与展望[J].自动化学报，2016，42(4)：481-494.

[13] 工业和信息化部信息中心.2018中国区块链产业白皮书[EB/OL].(2018-05-21)[2019-05-21].http://www.miit.gov.cn/n1146290/n1146402/n1146445/c6180238/part/6180297.pdf.

[14] 薛腾飞，傅群超，王枞，等.基于区块链的医疗数据共享模型研究[J].自动化学报，2017(9)：73-80.

[15] Bocek T，Rodrigues B，Strasser T，et al.Blockchains everywhere-a use-case of blockchains in the pharma supply-chain[C]//Integrated Network and Service Management，2017：772-777.

[16] Guan Zhitao，Si Guanlin，Zhang Xiaosong，et al.Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities[J].IEEE Communications Magazine，2018，56(7)：82-88.

[17] Elisa N，Yang L，Chao F，et al.A framework of blockchain-based secure and privacy-preserving e-government system[J].Wireless Networks，2018：1-11.

[18] Cebe M，Erdin E，Akkaya K，et al.Block4Forensic：an integrated lightweight blockchain framework for forensics applications of connected vehicles[J].IEEE Communications Magazine，2018，56(10)：50-57.

[19] Buterin V.On public and private blockchains[EB/OL].(2015-08-07)[2018-05-21].https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/.

[20] Hyperledger.Hyperledger fabric[EB/OL].[2019-05-21].https://hyperledger-fabric.readthedocs.io/en/latest/.

[21] Diffie W，Hellman M.New directions in cryptography[J].IEEE Transactions on Information Theory，1976，22(6)：644-654.

[22] 朱涛，姚翔，许玉壮，等.基于Fabric的跨境汇款追踪平台实现[J].信息安全学报，2018，3(3)：50-61.

[23] Yang Jian，Lu Zhihui，Wu Jie.Smart-toy-edge-computing-oriented data exchange based on blockchain[J].Journal of Systems Architecture，2018.

[24] Redis.Redis introduction[EB/OL].[2019-05-21].https://redis.io/topics/introduction.

[25] 马春光，安婧，毕伟，等.区块链中的智能合约[J].信息网络安全，2018，215(11)：13-22.