



研究与开发

基于区块链的生鲜奶供应链可信追溯系统方案

刘应, 范洪博, 马首群, 高志伟, 刘锦江

(昆明理工大学信息工程与自动化学院, 云南 昆明 650500)

摘要: 生鲜奶是我国奶业发展的重要方向, 溯源体系对整个生鲜奶行业的发展至关重要。时效性强、问题事后发现、受害者难以追踪、质检体系难以获得信任四大问题是生鲜奶行业区别于其他农产品行业的主要特征, 传统农业领域溯源机制甚至基于区块链的农产品溯源机制无法满足生鲜奶行业的溯源要求。设计了一种面向生鲜奶供应链体系的追溯系统方案 RMChain, 在满足现有区块链溯源机制的各种优点的同时, 针对生鲜奶特点进行专门的优化, 在用户溯源产品的同时, 也便于问题奶的追踪定位和消费者赔偿, 有效改善了生鲜奶行业的溯源现状。针对大文件严重影响区块链性能的问题, 设计了基于数据重要性的多方存储模式, 测试系统原型核心交易量性能数据表明, 系统访问性能明显提升, 验证了 RMChain 的可行性。

关键词: RMChain; 区块链; 生鲜奶; 多方存储; 准入机制

中图分类号: TP313

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2021103

Blockchain based trusted traceability system scheme for raw milk supply chain

LIU Ying, FAN Hongbo, MA Shouqun, GAO Zhiwei, LIU Jinjiang

Faculty of Information Engineering and Automation,
Kunming University of Science and Technology, Kunming 650500, China

Abstract: The development of raw milk is an important direction for the development of China's dairy industry, and a traceability system for the raw milk industry was proposed for the development of the entire industry crucially. The characteristics of the raw milk industry were analyzed and four major problems were proposed as the timeliness, the problems found after the fact, the difficulty in tracing the victims, the quality control system, such as difficulties in gaining trust, which were the main characteristics that distinguish the raw milk industry from other agricultural industries, and led to traceability in traditional agriculture. The mechanism or even the popular blockchain-based traceability mechanism for agricultural products could not meet the traceability requirements of the raw milk industry. Based on this finding, RMChain, a traceability system for raw milk supply chain system scheme, was designed to meet the requirements of the existing blockchain-based traceability mechanisms in the raw milk industry. In addition to the various advantages of the chain traceability mechanism, it was also optimized specifically for the characteris-

收稿日期: 2020-10-24; 修回日期: 2021-05-10

通信作者: 范洪博, 1105058257@qq.com

基金项目: 国家自然科学基金资助项目 (No. 41364002)

Foundation Item: The National Natural Science Foundation of China (No. 41364002)

tics of raw milk, which made it easy for users to trace the product and facilitate the traceability of the milk. The tracking and location of problem milk and consumer compensation effectively improved the traceability status of the fresh milk industry. For the problem of large files seriously affecting the performance of the blockchain, a multi-party storage model based on the importance of data was also designed. The feasibility of RMChain was verified.

Key words: RMChain, blockchain, raw milk, multi-party storage, access mechanism

1 引言

在各种奶类产品中,生鲜奶因其营养价值高、口感好、附加值大等特性,是我国奶类产业发展的重点,智研咨询发布的《2020—2026 年中国鲜奶行业市场研究分析及投资策略探讨报告》的数据显示:2019 年,中国鲜奶销售额/(鲜奶+常温白奶销售额)比值仅为 26.71%,英国、澳大利亚、日本、美国对应比值分别为 94.15%、88.67%、98.30%、98.22%,这些数据体现了全球生鲜奶行业增长的潜力与空间。

中国是奶制品安全问题凸显的国家,其中大头娃娃奶粉^[1]、黄曲霉毒素、三聚氰胺等事件^[2],对中国的奶制品行业造成了难以挽回的损失,也严重影响了消费者的消费欲望。特别在生鲜奶领域,由于生鲜奶要求就近生产、就近消费,消费者周围主要的奶源为中小型奶场等,消费者对这些中小型奶场的奶制品的食品安全能力难以把控。传统溯源体系建设中,要求所有的生产者、供应链、消费者均要完全相信溯源系统建设方,造成了昂贵的信用成本,同时,中心化的溯源信息管理可能被篡改、被伪造,不仅损害了生产者的利益,还威胁人们的身体健康^[3],且存在数据平台运营费用高昂、信息录入不及时、追踪信息不全面等诸多弊端。

2008 年,伴随着比特币出现了区块链技术^[4],记录在区块链上的信息具有几乎不可篡改、数据永久公开透明可追溯、去中心化等优势,已被证明是最优的溯源体系底层技术。2019 年 5 月,国务院发布的《关于深化改革加强食品安全工作的意见》中明确指出,推进区块链等技术在食品安

全监管领域的应用,实施智慧监管,2020 年中央一号文件中指出,加快区块链等现代信息技术在农业领域的应用。

本文分析了生鲜奶行业的特性,针对生鲜奶行业特点,分析该领域和传统农产品溯源领域的重要区别,并进行了针对性的设计,利用超级账本技术 Fabric 区块链,设计了一种专门针对生鲜奶行业的溯源系统 RMChain,该系统在保持区块链技术几乎不可篡改、低成本信用等优势上^[5],有效针对生鲜奶的强时效性和问题事后暴露等特点,使用密码学区块链中的信息确保信息安全^[6],进行专门的溯源跟踪。

2 生鲜奶溯源中的问题

(1) 生鲜奶具有强时效性

经过的加工程序不同,保存的环境不同,鲜奶的保质期时间的长短也会有所不同,具体要分情况而论。

未经过加工处理的生鲜牛奶,即刚挤出来的牛奶,一般可以保存 24~36 h。经过巴氏杀菌处理的鲜奶,一般可以保存 1~2 周的时间。经过超高温杀菌技术处理的牛奶,储存方便且保质期会比较长,本文所描述的生鲜奶主要指这种牛奶。

(2) 遇问题常呈现事后暴露的情况

在生鲜奶中,常出现霉菌、金黄色葡萄球菌等感染情况^[7-8],这些微生物感染将对饮用者造成严重的健康威胁,现有的沙门氏菌快速检测技术也经常要超过 24 h 才能有检测结果^[9]。而由于生鲜奶只有 24~36 h 的保质期,当检测发现奶中存在问题时,消费者已经把问题奶饮



用掉了。

(3) 问题生鲜奶难以追踪

奶类产品是液体,无法在奶中加入传感器、快速检测技术等溯源信息收集装置,典型的瓶装生鲜奶,因奶瓶无法供电,无法安装GPS定位等手段,也难以对奶的销售流向进行数据追溯^[10]。

(4) 监管难以事后介入

生鲜奶的强时效性导致了监管部门事后介入时,主要的有效质量数据已经难以追踪。应在生鲜奶销售就近建立大量微型质量检测网络,确保每个厂商每个批次的奶都有对应的质量检测报告。

以上4点问题是生鲜奶溯源行业与传统农产品溯源行业的主要区别,现有基于商品的溯源体系(哪怕是区块链溯源体系)难以满足生鲜奶行业的溯源需求,必须进行针对性的设计。

3 区块链溯源

区块链技术的出现为供应链管理引入了一种新的思维方式^[11-14],是一种去中心化的方案^[15],在生鲜奶供应链中,信息的可溯性是涉及生产和分配商品的所有过程的连接,从原材料到制成品再到最终的消费者,其牛奶的可追溯性系统可以定义为一种能够保证生鲜奶在整个供应链中的运行可以被追踪的系统^[16]。

基于区块链的可追溯性系统的想法最早于2015年11月出现,Alexis Bateman认为^[17],由于缺乏标准化,区块链将是解决跨供应链信息挖掘和管理挑战的现实技术选择,区块链技术可以确保对鲜奶链中的每个批次进行可靠的跟踪。在发现食源性疾病的情况下,区块链可以很容易地找到有缺陷的产品并丢弃所有受影响的产品批次。目前,市场上已有美国最大牛奶公司Dairy Farmers of America与食品科技公司ripe.io展开合作,拟利用后者开发的区块链来追踪奶源、

提升数据透明度,以此提高消费者对于鲜奶安全的信心。

食品可追溯性已被视为确保食品安全和高质量的重要方面^[18],根据Deloitte的调查,2019年消费品和制造业的公司中有42%计划在区块链技术上花费至少500万美元。而在参考文献[19]中,在供应链管理中的区块链预计将以87%的年增长率增长,到2023年预计将从2018年的4500万美元增加到3.346亿美元。区块链提供了不可更改的交易记录,所有生产产品和运输详细信息均通过不同的技术收集并经过验证,在区块链账本上永久记录^[20],区块链可追溯系统具有去中心化的特点,并采用可靠的技术方法来记录生鲜奶中的可追溯数据并存储在共同的账本上,通过智能合约保障交易的安全性^[21-23],而且监管机制也能参与整个过程,能在生鲜奶供应链中对数据溯源起到至关重要的作用。

4 RMChain 系统模式

4.1 多方存储加速机制

本系统大量涉及检测报告等较大的数据,传统区块链溯源系统中,所有数据都放在区块链中,由于区块链账本相对昂贵且性能较低,各种数据放在一起的方式严重影响了系统的并发能力和吞吐率。参考文献[24]提出etherQL系统,该系统在区块链之外设计了一个单独的查询层,将区块链的原始数据复制到外部数据库,提高查询效率。本系统中在此思想上,运用多方存储分离存储的加速机制,同时保障了数据的快速访问和不可篡改性。

系统所有加入的数据可以根据其重要性进行分级。对于产品保质期、各方基本数据等在用户查看数据时必须第一时间就要确保正确的数据,数据直接存储在Fabric网络中。而对用户非重要的数据(如奶牛的检测报告、企业的资质文件等),无须存储在较为昂贵的区块链中,区块链中只存

储非重要数据 Hash 值,并将非重要数据同时存储在访问速度较快的云数据库和相对访问较慢但难以篡改的 IPFS 区块链中。其中,IPFS 也是一种面向文件存储的区块链技术,虽然没有智能合约等相关技术支持,但 IPFS 能快速存储一些较大数据,其存储数据几乎不可篡改。

目前用户和企业都倾向于将数据存储在云端服务器,但并没有经过加密处理,虽然提供了诸多便利,但仍存在各种安全问题^[25],本文的多方存储查询方式如图 1 所示,基于数据的重要性,用户查看非重要数据时,通过异步查询方式,数据由云数据库提供,在向用户展示前,先计算其 Hash 值,并与 Fabric 中记录数据进行比对。若比对通过,则证明云数据库中数据没有被改动,可以向用户展示;若比对失败,则将云数据库中的数据作废,从 IPFS 区块链中下载真实数据并展示。通过这种交叉访问的方式,在保障区块链几乎不可篡改的特性的同时,

又有云数据库的高速访问能力,可明显提高区块链性能。

4.2 系统架构

RMChain 主要由 UI 层、管理层、数据层(链外)和区块层(链上)组成,区块链用作包含数据和业务逻辑的软件连接器,涉及 6 个不同类型的用户。

- 生产方:奶牛牧场提供生鲜奶,并进行灌装包装等必要加工。
- 运输方:负责生鲜奶的运输、仓储的运输方,考虑到物流端方便管理,系统引入了 RFID 辅助二维码进行运输端数据的管理。
- 销售方:负责进行生鲜奶销售。
- 质量监控网络:第三方质检企业,对生鲜奶质量进行质检,出具质检报告。
- 消费者:购买生鲜奶,需要了解生鲜奶的全流程,并在出现问题时获得赔偿。
- 监管方:对整个系统数据进行管理。

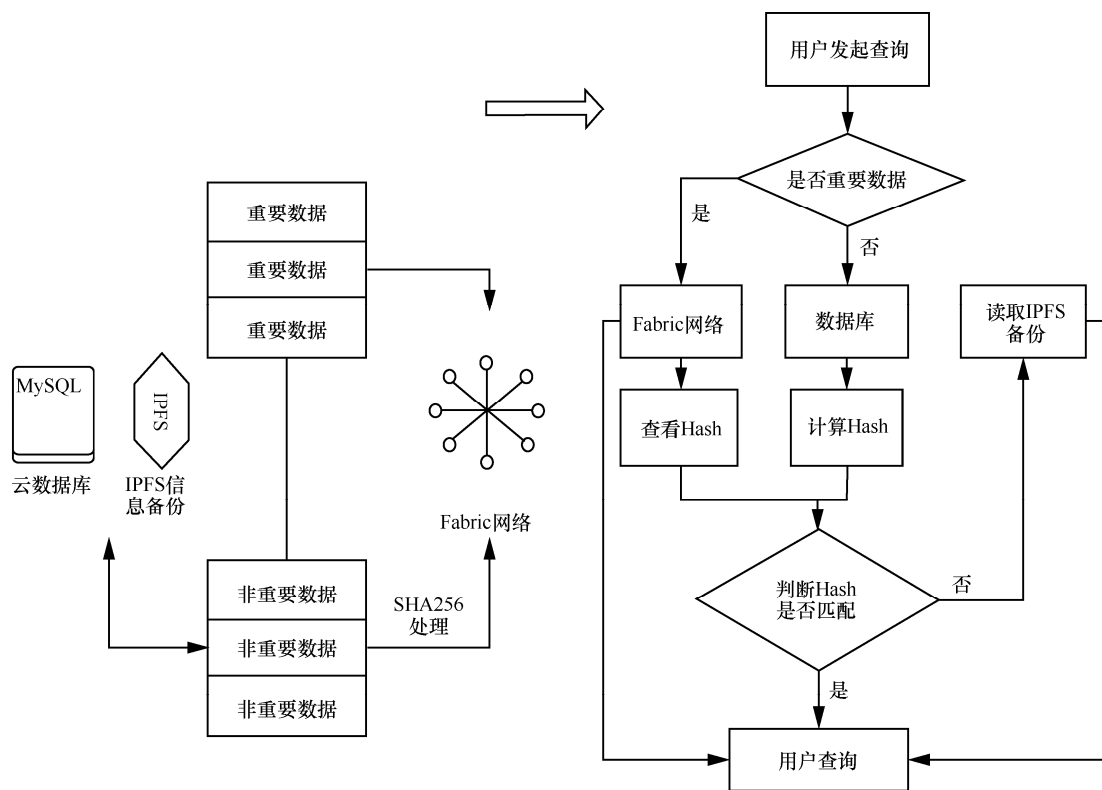


图1 多方存储查询方式



系统采用 Hyperledger Fabric 搭建联盟链作为区块链网络,其位于公共区块链和私有区块链之间,且都是通过独特的结构确保数据的难以篡改性^[26],用于同时存在多个用户角色,在本节的 RMChain 模型,用于整个生鲜奶供应链平台的追溯以及认证,其目标是监视生鲜奶供应链信息的整个过程,其体系结构如图 2 所示。

系统中,通过准入机制,所有用户提前在本系统 CA 中进行注册认证,获得访问区块链系统的唯一私钥,并由客户端基于私钥,经不可逆计算,生成用户公钥和对外二维码,对外二维码中包含了公钥信息,该二维码用于系统间的身份认证和数据交互。

用户在注册时,需实名注册,提交身份证、个人联系方式、地址等必要信息,若是企业还需提供企业资质凭证,凭证不能通过审核者,CA 拒绝向其发放私钥。

在整个生鲜奶的生产、消费、监管过程中,系统的交互模式如图 3 所示。

步骤 1 生产端生产生鲜奶,并完成奶质自查,形成检测报告,系统根据当前批次,生成唯一的批次 ID 以及和瓶身绑定的溯源码 ID,生产端在系统中输入批次 ID 和批次信息,包含(生产时间地点、奶牛信息、批次产量、生产端自检检测报告等)上链,并利用生产端私钥对所录入的信息进行数字签名。根据批次产量,生成唯一的瓶身溯源二维码和 RFID 信息。瓶身溯源二维码有可刮开的密码区,生产端在瓶身张贴溯源二维码,在包装箱中加入已写数据的 RFID,每瓶溯源二维码对应数据和批次数据进行绑定,RFID 数据和包装箱内各瓶生鲜奶溯源二维码对应数据进行绑定。

步骤 2 运输端对已经张贴溯源二维码和 RFID 的生鲜奶进行仓储和运输,通过读写 RFID 的数据,输入运输时间、经手人、运输源、目的地、出入库信息、仓储信息等信息,数据上链并利用运输端私钥对输入数据进行数字签名。

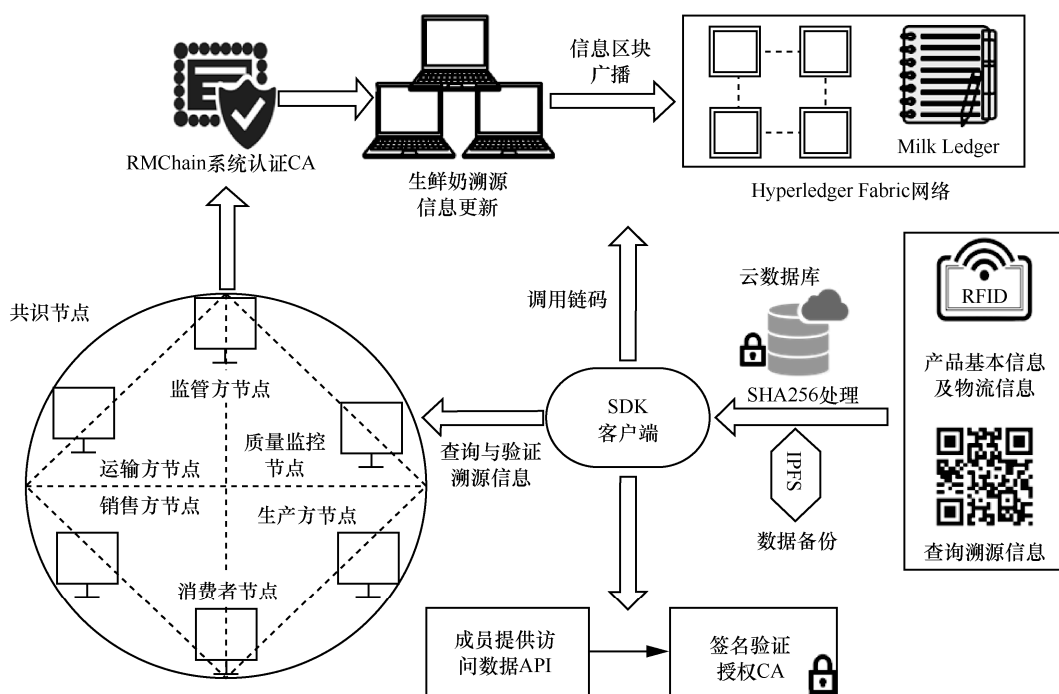


图 2 RMChain 系统架构

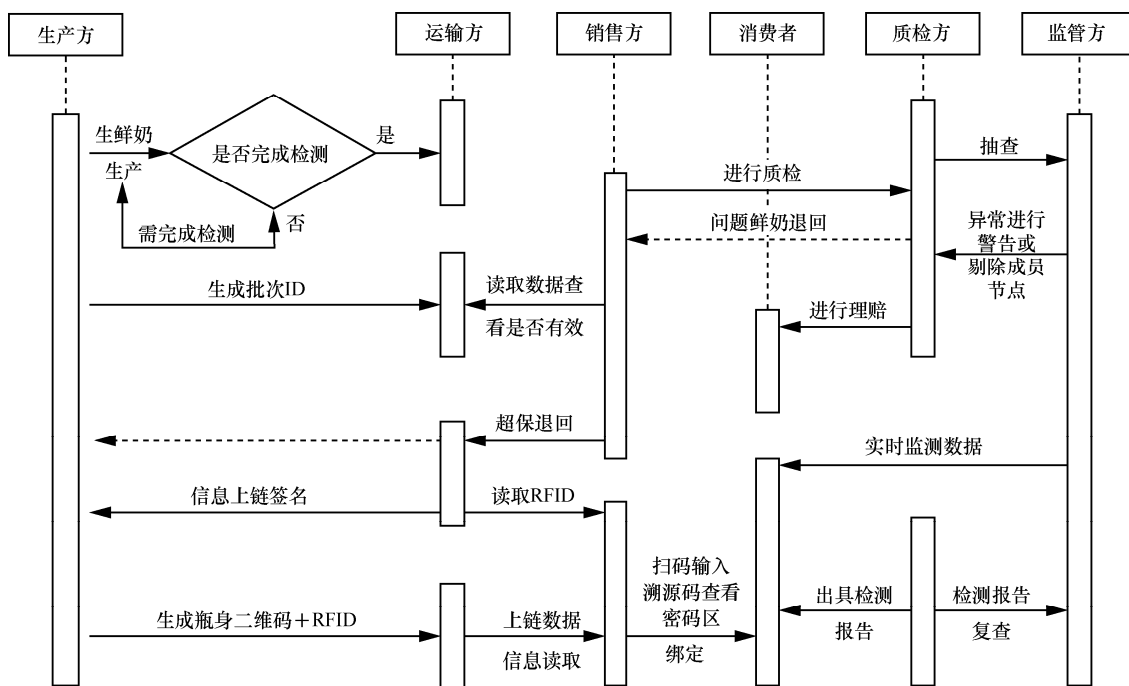


图3 数据交互图

步骤3 销售端利用RFID数据,完成产品的上架销售工作,上架过程输入上架时间、销售资质、销售方式等信息,数据上链并数字签名。根据数据录入的时间戳,系统实时提醒本批次生鲜奶还能销售的时间段,销售端对超保质期的生鲜奶可以直接拒收。当超出保质期时限后,要求厂商根据区块链记录销售情况,将剩余未销售的生鲜奶进行回收销毁,销毁数据登记到区块链。

步骤4 消费者在购买生鲜奶时,扫描瓶身溯源二维码,在通过输入溯源码即可查看步骤1~步骤3所录入的所有信息,并由系统自动验证所有信息的数字签名,确保信息的实名录入。若消费者认可这些产品的溯源信息,需要进行购买时,要求刮开密码区,并在系统中输入密码,输入密码后,即完成了消费者和对应生鲜奶的绑定,绑定关系上链,并由消费者自身私钥进行数字签名。该绑定关系也是当生鲜奶出现质量问题后,作为赔偿的凭证。

步骤5 每批次的生鲜奶要求送样品给指定

第三方检测机构进行质量检测,质量检测报告绑定每批次的生鲜奶,在检测报告完成时,上链并由第三方检测机构数字签名,检测报告推送购买本批次生鲜奶的用户,让消费者能及时了解生鲜奶的质量问题。若检测到沙门氏菌等问题,告知用户就医方案和赔偿方案,让用户有所准备。检测报告由监督部门进行复查,杜绝检测机构乱出检测报告的可能。

步骤6 监督部门监控链上数据,对各方进行现场抽查、数据复查和审计,并在出现问题时进行有效协调,对出现问题或违规的各方,进行警告处理,剔除节点,严重者将通过记录数据的信息追究法律责任。

4.3 算法步骤

根据参与者角色功能的制定,每个参与方只有执行背书策略后的每笔交易才有效,其相关算法如下。

算法1 生成生鲜奶溯源信息

在算法1中定义监管部门为MP,各参与方信息为GE,生产方信息为I,运输方信息为LO,销



售方为 SE, 检测方信息为 TE, 其生产方生产完后提供每批生产的批次号 ID 以及溯源号 MilkID, 下面为智能合约如何将生鲜奶的基本信息打包成区块以及数据存储过程。

输入 MilkID,GE

输出 MP_Message,TE

步骤 1 判断输入参数正确性, 如果输入数据不满足设定数据参数值, 则返回错误, 若参数输入正确, 则判断其溯源 ID (溯源 MilkID $\in$ 批次 ID) 是否存在, 若存在则获取正确的溯源信息, 反之则返回错误, 对拿到的数据进行处理如下:

(1) Json.Unmarshal for I/LO/SE/TE //对数据信息反序列化*/

(2) GE.Generate(W) $W \in I/LO/SE/TE$ //生成相关区块数据*/

(3) select $W1 \rightarrow networks(W1 \in W$ 为重要数据) /*将重要数据存储区块链*/

(4) select $W2 \rightarrow central\ database(W1 \in W$ 为非重要数据)/*将非重要数据存储数据库*/

(5) $W \rightarrow IPFS$ //将数据备份到 IPFS

步骤 2 各方参与信息对生成的数据进行签名 (signature) 并生成 CA 发送给 MP 进行审核, MP 验证签名和 CA 无误后则审核通过, 生成监管信息 MP_Message; TE 进行链上标记是否通过, 未通过将通知相关参与方整改, 严重者启动法律程序。

算法 2 通过 MilkID 追溯数据信息

输入 MilkID

输出 I,LO,SE,TE,MP_Message

步骤 1 通过关键的 MilkID 查询生鲜奶的基本信息并追溯数据的历史记录。

步骤 2 通过 MilkID 查询并返回 I/LO/SE/TE 各方的数据结果并使用 GetState 方法写入查询区块信息记录。

步骤 3 通过数据库中数据计算 SHA256 值, 其结果 Hash A 和 Fabric 网络中存储的 Hash B 的结果做对比, 其操作如下:

(1) get Hash Result A from Fabric //获取哈希 A 的信息

(2) Json.Unmarshal for I/LO/SE/TE //进行反序列化

(3) query data B from CentralDB and applying SHA256 /*获取数据库数据计算哈希*/

(4) Comparison HASH Results A and B /*A 与 B 哈希结果对比判断是否篡改*/

(5) If data $B \neq A$, return err $\rightarrow MP$ /*数据被篡改, 返回错误提交给监管方*/

(6) applying IPFS data //请求匹配存在 IPFS 中的数据备份*/

(7) else continue //若没被篡改继续执行下一步

步骤 4 通过 GetHistory 追溯历史数据放入迭代器中。

步骤 5 对查询到的历史数据, 查看 I、LO、SE、TE、MP_Message 数据来实现数据追溯。

算法 3 监管部门监管账本信息 (超级管理员)

输入 admin,MilkID

输出 MP_Message

步骤 1 参与者通过准入机制向 MP 申请注册 CA 分发公钥和私钥成为账本参与节点。

步骤 2 MP 有对账本进行重要操作的权限, 除了算法 2 中的相关权限以外, 其他权限操作如下:

(1) get data from Fabric and CentralDB from I/LO/SE/TE

(2) update / removedata $\rightarrow block$ I/LO/SE/TE /*若果发现信息有误可以从区块链上及时更新和删除节点信息, 区块会记录所有操作记录*/

(3) MP audit I/LO/SE/TE //对所有数据进行审查和复查

步骤 3 如果发现违规, 将执行算法 1 的步骤 2。

5 实验与分析

5.1 实验结果

本次溯源链均通过平台注册参与方用户获得

相应的 CA 和私钥, 成员身份基于标准的 X.509 证书, 密钥使用的是 ECDSA 算法, 利用 PKI 体系给每个参与方颁发数字证书, 均授权访问 RMChain。根据实验生产商初始化信息假设将批次为 P/N202008 并绑定批次号溯源编号 XN20200702 和 XN20200920 的生鲜奶提供给运输方甲方, 可扫码后通过输入溯源号码查询溯源信息, 通过数据库查询并进行 Hash 比对, 若正确, 则追溯成功。

测试采用系统为 64 bit 的 Ubuntu18.04、处理器为 Intel Core i5 (2.7 GHz)、内存为 8 GB 的设备进行运行测试, 并在 Docker 虚拟容器环境运行, 采用 Fabric-sdk-go 进行客户端开发, 设定了两个 Org 组织, Org1 为监管方、质量监控方以及消费者组成的监督节点, Org2 为运输方、生产方、销

售方、消费者的源数据组织, 通过超级管理员进行权限控制, 共有 3 个 peer 节点, 两个 CA 节点认证进行测试。

图 4 为生鲜奶追溯客户端实现, 其生产端管理员数据接入部分上链流程。其用户查询包含各节点管理员更新的数据信息记录以及关键数据信息, 包括部分生产、运输、质检、销售信息。

5.2 交易性能处理分析

Hyperledger caliper 是用于区块链网络的基准测试工具, 它支持各种超级账本框架, 通过对于此次试验交易处理时间内交易的 RMChain 系统成员(生产方、运输方、销售方、检测方、消费者、监管方)的每轮写入超级账本的网络交易次数进行了相关的性能测试, 其交易时间决定了区块链的性能。


加密、安全、信赖
 TRACEABILITY OF RAW MILK 您身边的放心牛奶

[网站首页](#)
[数据接入](#)
[溯源查询](#)
[成功案例](#)
[用户中心](#)
[在线留言](#)
[管理端入口](#)
[注册/登录](#)

生产端添加生鲜奶生产数据信息

[返回首页](#)

生鲜奶溯源码: XN20200702	加工方式: 巴氏杀菌处理
批次号: P/N202008	执行标准: 国家标准
录入管理员: 小刘	批次产量: 40吨
保质期: 36小时	运输物资: 罐车
鲜奶价格: 45.00/瓶	检测报告: QmDbgl.wHVDCSIAKVN1B4r6zTX
生产地点: 云南昆明	备注信息: 暂无



[Add milk information](#)

生产端添加生鲜奶生产数据信息

[返回首页](#)

产品数据信息添加成功, 区块交易hash为: fa546e1f0ebe8394ecec5c27c3e0289b6fa5b5b8a1188e5c6ac2b7abd7fa9d44

生鲜奶信息查询结果

溯源码	批次号	鲜奶价格	保质期	生产地点	加工方式	批次产量	运输物流	储藏方式	时间戳
XN20200702	P/N202008	50.00/瓶	36小时	内蒙古	巴氏杀菌	30吨	顺丰	冷链	2020-10-24 10:15:36
XN20200920	P/N202008	50.00/瓶	36小时	内蒙古	超高温杀菌	30吨	顺丰	冷链	2020-10-24 10:16:43
XN20200920	P/N202008	50.00/瓶	36小时	新疆	超高温杀菌	30吨	速运	冷链	2020-10-24 10:17:52

溯源码: XN20200920

检测报告: QmPxHN8TYZQhmzj***

质检报告: QmRFw6kRRxymugT***

鲜奶价格: 50.00/瓶

执行标准: 国家标准

加工方式: 超高温杀菌

运输时间: 2020-10-24

运输时间: 2020-10-24

复查情况: 1e9f2561b7cf43c49***

运输单号: 202010246561

运输物流: 速运

RFID是否绑定: 绑定

运输目的地: 云南昆明

销售数据: 1e9f2561b7cf43c49***

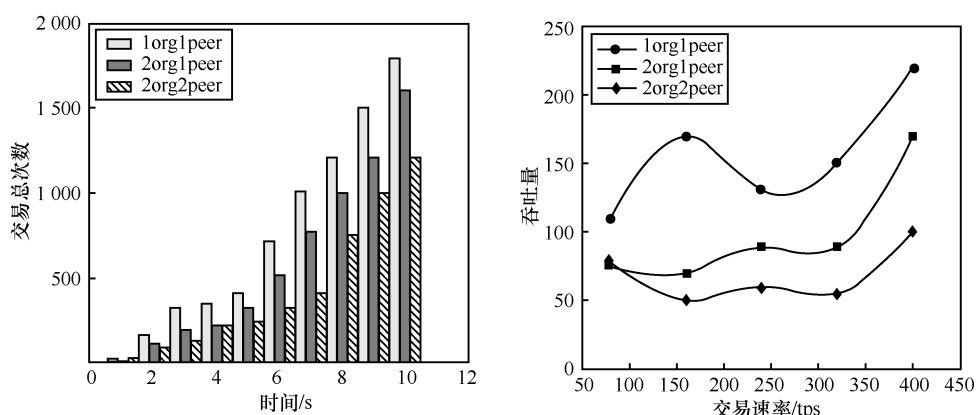

[更新追溯信息](#)
[返回首页](#)

图 4 生鲜奶追溯实现

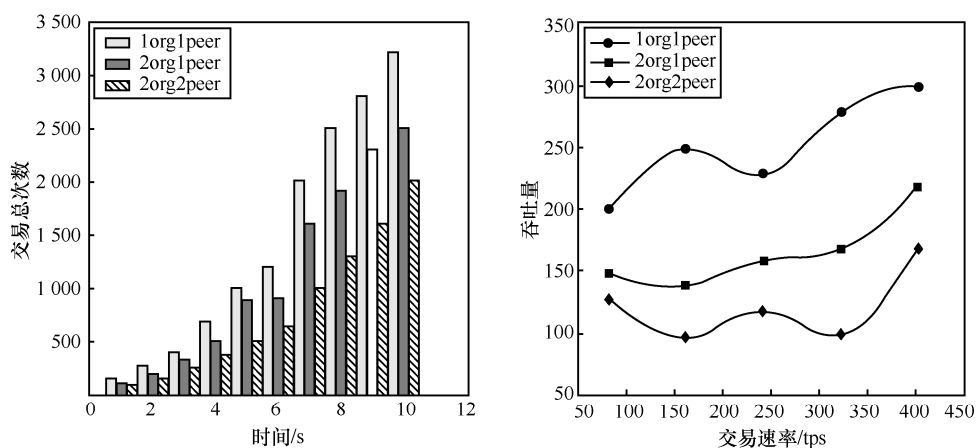


按每次执行 1 000 笔交易, 交易速率为 80、160、240、320、400 笔交易每秒 (tps), 如图 5 所示, 显示了不同的网络中配置交易所需花费的必要时间, 其中包含在网络的异常配置中成功完成事务所花费的时间。在 1org1peer、2org1peer、

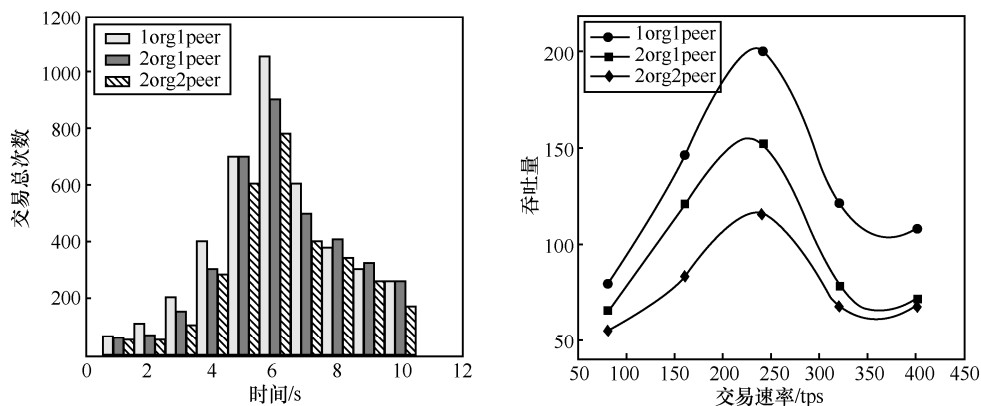
2org2peer 中, 表示不同的性能, 经过 5 轮测试, 每轮 1 000 笔交易, 在 10 s 后, 在 Fabric 网络自带 couchDB 中 1org1peer 完成 1 800 笔交易, 2org1peer 达到 1 610 笔交易, 而 2org2peer 达到 1 200 笔交易。同样, 在数据不被篡改的情况下



(a) couchDB交易时间以及吞吐量与交易速率之间的关系



(b) MySQL交易时间以及吞吐量与交易速率之间的关系



(c) IPFS交易时间以及吞吐量与交易速率之间的关系

图 5 RMChain 性能测试

couchDB+MySQL 中 1org1peer 完成 3 200 笔交易, 2org1peer 达到 2 511 笔交易, 而 2org2peer 达到 2 000 笔交易, 数据明显提升, 所以随着组织的增加, 执行交易的时间也同样增加了。而在数据被篡改的情况下, 在启用 couchDB+IPFS 备份可以看到性能有所下降, 最高在 1 000 笔交易量时作用, 这是由于随着交易量增加, 达到一定数量时 IPFS 就会出现延迟。

同样在图 5 中吞吐量与交易速率之间也有所体现, 其用 MySQL 的 1org1peer 可到 300 tps, 而 2org1peer 和 2org2peer 将吞吐量分别降低到 200 tps 和 150 tps。这显示了更高的时延, 并带来了通信间隙, 以实现更好的性能, 而在数据篡改的情况下交易量也同样降低, 这是由于 IPFS 文件较多时缓冲较慢但可保障数据的真实性, 在其保证消费者能够查看正确信息的同时, 监管方会介入查询被篡改对象进行相应追责。

通过本次实验可以得出: 区块链技术能有效地解决传统供应链溯源项目中的伪造、掺假等问题, 包括如下几点。

(1) 对于具有强时效性的问题, 图 4 以及实验分析可以看出用户对生鲜奶进行校验时, 会进行时间戳的记录, 通过记录的时间戳系统可以进行时效性的追踪, 就可以判断哪些鲜奶到用户手中过了有效期。

(2) 对于遇到问题后无法追踪以及事后暴露等问题, 通过区块链对数据的实时记录更新, 其中那个负责的数据参与方就会追踪到参与者。可以通过出问题的产品溯源 ID, 找到参与者的生产方、检测方等责任人。

(3) 目前的溯源体系都是事后的监管介入, 本次设计的联盟区块链、监管方节点和质量监管节点均已加入联盟组织, 可以对上链的数据进行实时的监管, 如果发现问题就会进行节点的剔除和追责, 监管方作为超级管理员的角色具有授权、剔除、审核等权限, 可以由专门的政府监管部门或者企业监

管部门参与。

通过实验分析, RMChain 系统可以实现整个供应链生鲜奶信息的可追溯性以及安全性, 由于区块链系统每次交易都有签名和证书且分布在各个节点上同时进行账本的更新和记录, 因此 RMChain 具有很好的防篡改能力以及每个参与方在系统级的隐私保护和信息分散化方面具有一定的优势。

6 结束语

区块链溯源是农产品溯源的必然发展方向, 其广泛应用对整个农业发展具有重要的意义。本文所提出的 RMChain 生鲜奶供应链溯源体系, 针对生鲜奶行业的特点进行有针对性的改进和优化, 展示了较强的可行性和可落地性, 联盟链作为底层架构许可节点的加入, 可以保障数据质量的安全性, 为区块链在其他领域中的广泛应用提供了一定的借鉴意义。

本文对于上链前的数据采用 RFID 作为保障进行系统方案设计, 区块链则保证上链后的数据无法篡改, 目前区块链技术必须结合物联网以及其他技术保障上链前数据的不可篡改性。区块链技术目前作为国家“新基建”在高速发展中, 每秒百万级别交易的区块链系统、更灵活高效的智能合约系统、区块链预言机 (Oracle 自动验证上链数据的正确性) 等研究正在不断地突破。随着这些技术的落地和完善, 未来区块链的应用范围将更加广泛, 区块链技术将更深层次地改变现实生活的底层逻辑。

参考文献:

- [1] 罗志华. “大头娃娃”再敲儿童食品安全警钟[J]. 浙江人大, 2020, 6(6): 79.
LUO Z H. Big-headed dolls alarming children's food safety again[J]. Zhejiang NPC, 2020, 6(6): 79.
- [2] 张薇薇. 我国牛奶安全存在的问题及应对策略[J]. 食品安全导刊, 2018(27): 40.
ZHANG Y W. Problems and coping strategies of milk safety in China[J]. Food Safety Ledger, 2018(27): 40.



- [3] 安瑞, 何德彪, 张韵茹, 等. 基于区块链技术的防伪系统的设计与实现[J]. 密码学报, 2017, 4(2): 199-208.
AN R, HE D B, ZHANG Y R, et al. The design of an anti-counterfeiting system based on blockchain[J]. Journal of Cryptologic Research, 2017, 4(2): 199-208.
- [4] BHARDWAJH S, KAUSHIK M. Blockchain-technology to drive the future[J]. Smart Innovation, 2018, 10(28): 263-271.
- [5] YLI-HUUMO J, KOD, CHOI S, et al. Where is current research on blockchain technology?-A systematic review[J]. PLoS One, 2016, 11(10): e0163477.
- [6] LI T C, SUN S D, BOLIĆ M, et al. Algorithm design for parallel implementation of the SMC-PHD filter[J]. Signal Processing, 2016(119): 115-127.
- [7] BURITI F C A, CARDARELLI H R, SAAD S M I. Biopreservation by *Lactobacillus paracasei* in coculture with *Streptococcus thermophilus* in potentially probiotic and synbiotic fresh cream cheeses[J]. Journal of Food Protection, 2007, 70(1): 228-235.
- [8] FAVARO L, BARRETTO PENNA L, TODOROV S D. Bacteriocinogenic LAB from cheeses - application in biopreservation?[J]. Trends in Food Science & Technology, 2015, 41(1): 37-48.
- [9] CLAEYS W L, CARDOEN S, DAUBE G, et al. Raw or heated cow milk consumption: review of risks and benefits[J]. Food Control, 2013, 31(1): 251-262.
- [10] MYLAN J, GEELS F W, GEE S, et al. Eco-innovation and retailers in milk, beef and bread chains: enriching environmental supply chain management with insights from innovation studies[J]. Journal of Cleaner Production, 2015(107): 20-30.
- [11] DUAN Y, EDWARDS J S, DWIVEDI Y K. Artificial intelligence for decision making in the era of big data - evolution, challenges and research agenda[J]. International Journal of Information Management, 2019, 48(10): 63-71.
- [12] 白小宇, 王莹, 贾敬敦, 等. 区块链技术在农产品质量安全追溯体系中的应用设想[J]. 中国植保导刊, 2019, 39(3): 90-93.
BAI X N, WANG Y, JIA J D, et al. Application of blockchain technology in agricultural product quality and safety traceability system[J]. China Plant Protection Journal, 2019, 39(3): 90-93.
- [13] QUEIROZ M M, FOSSO WAMBA S. Blockchain adoption challenges in supply chain: an empirical investigation of the main drivers in India and the USA[J]. International Journal of Information Management, 2019, 46(6): 70-82.
- [14] WANG Y, HANJH, BEYNON-DAVIES P. Understanding blockchain technology for future supply chains: A systematic literature review and research agenda[J]. Supply Chain Management: An International Journal, 2019, 24(1), 62-84.
- [15] 杨慧琴, 孙磊, 赵西超. 基于区块链技术的互信共赢型供应链信息平台构建[J]. 科技进步与对策, 2018, 35(5): 21-31.
YANG H Q, SUN L, ZHAO X C. Build mutual trust supply chain information system based on blockchain[J]. Science & Technology Progress and Policy, 2018, 35(5): 21-31.
- [16] DABBENE F, GAY P, TORTIA C. Traceability issues in food supply chain management: a review[J]. Biosystems Engineering, 2014(120): 65-80.
- [17] BATEMAN A H. Tracking the value of traceability[J]. Supply Chain Manag Rev, 2015: 8-10.
- [18] RESENDE-FILHO M A, HURLEY T M. Information asymmetry and traceability incentives for food safety[J]. International Journal of Production Economics, 2012, 139(2): 596-603.
- [19] XU X W, PAUTASSO C, ZHU L M, et al. The blockchain as a software connector[C]//Proceedings of 2016 13th Working IEEE/IFIP Conference on Software Architecture (WICSA). Piscataway: IEEE Press, 2016: 182-191.
- [20] 周登极, 谢明. 区块链技术在金融领域的应用前景研究[J]. 中国市场, 2017(34): 32.
ZHOU D J, XIE M. Research on the application prospect of blockchain technology in the financial sector[J]. China Market, 2017(34): 32.
- [21] 刘敖迪, 杜学绘, 王娜, 等. 区块链技术及其在信息安全领域的研究进展[J]. 软件学报, 2018, 29(7): 2092-2115.
LIU A D, DU X H, WANG N, et al. Research progress of blockchain technology and its application in information security[J]. Journal of Software, 2018, 29(7): 2092-2115.
- [22] 蔡维郁, 郁莲, 王荣. 基于区块链的应用系统开发方法研究[J]. 软件学报, 2017, 28(6): 1474-1487
CAI W D, YU L, WANG R. Research on blockchain-based application development method[J]. Journal of Software, 2017, 28(6): 1474-1487.
- [23] WEBER I, XU X, REGISR, et al. Untrusted business process monitoring and execution using blockchain[M]//Business Process Management. Heidelberg: Springer International Publishing, 2016.
- [24] LI Y, ZHENG K, YAN Y, et al. EtherQL: a query layer for blockchain system[C]//Proceedings of International Conference on Database Systems for Advanced Applications. [S.l.:s.n.], 2017: 556-567.
- [25] 翁昕耀, 游林, 蓝婷婷. 基于区块链的结果可追溯的可搜索加密方案[J]. 电信科学, 2019, 35(9): 98-106.
WENG X Y, YOU L, LAN T T. Blockchain-based result-traceable searchable encryption scheme [J]. Telecommunications Science, 2019, 35(9): 98-106.

- [26] LEI K, ZHANG Q C, XU L M, et al. Reputation-based Byzantine fault-tolerance for consortium blockchain[C]//Proceedings of 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS). Piscataway: IEEE Press, 2018: 604-611.



马首群（1994- ），男，昆明理工大学信息工程与自动化学院硕士生，主要研究方向为区块链与信息安全。

[作者简介]



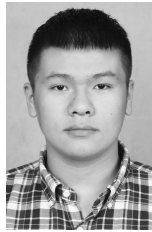
刘应（1994- ），男，昆明理工大学信息工程与自动化学院硕士生，主要研究方向为区块链与信息安全。



高志伟（1998- ），男，昆明理工大学信息工程与自动化学院硕士生，主要研究方向为区块链大数据。



范洪博（1982- ），男，博士，昆明理工大学信息工程与自动化学院讲师，主要研究方向为区块链、信息安全、互联网金融、密码学等。



刘锦江（1997- ），男，昆明理工大学信息工程与自动化学院硕士生，主要研究方向为区块链、大数据、神经网络等。