

基于区块链的粮油食品全供应链信息安全管理原型系统

许继平^{1,2} 孙鹏程¹ 张新^{1,2} 王小艺^{1,2} 孔建磊^{1,2} 赵峙尧^{1,2}

(1. 北京工商大学计算机与信息工程学院, 北京 100048;
2. 北京工商大学北京市食品安全大数据技术重点实验室, 北京 100048)

摘要: 粮油食品供应链具有全生命周期长、环节复杂、危害物种类多、信息多源异构等特点。基于区块链技术构建了一种新型的粮油食品供应链信息安全管理模型,研究并提出适用于粮油食品供应链的双模数据存储机制和管理供应链信息的智能合约,以保证信息存储和传输的安全可靠。在此基础上,基于 Hyperledger Fabric 设计了一种粮油食品全供应链信息安全管理原型系统,该系统能够实现粮油食品全供应链信息采集、查询、监控、追溯等功能,并通过具体的应用案例进行了验证和分析。

关键词: 粮油食品; 全供应链; 信息安全; 区块链; 超级账本; 智能合约

中图分类号: S126; TP391 文献标识码: A 文章编号: 1000-1298(2020)02-0341-09 OSID: 

Prototype System of Information Security Management of Cereal and Oil Food Whole Supply Chain Based on Blockchain

XU Jiping^{1,2} SUN Pengcheng¹ ZHANG Xin^{1,2} WANG Xiaoyi^{1,2} KONG Jianlei^{1,2} ZHAO Zhiyao^{1,2}

(1. School of Computer and Information Engineering, Beijing Technology and Business University, Beijing 100048, China
2. Beijing Key Laboratory of Big Data Technology for Food Safety, Beijing Technology and Business University, Beijing 100048, China)

Abstract: The cereal and oil food supply chain is characterized by long full life cycle, complicated links, diversified hazardous materials and multi-source heterogeneous information. The cereal and oil food full supply chain information security management prototype system based on blockchain was put forward, which stored and managed the multi-source heterogeneous cereal and oil food supply chain information via the tamper-proof and information-traceable features of blockchain. Through business process analysis of cereal and oil food supply chain, its new-type information security management model was built based on blockchain technology, the dual-mode data storage mechanism suitable for it was studied and proposed, the supply chain data was stored by the combination of blockchain storage and off-chain database storage. In addition, the supply chain information was managed through the smart contract, ensuring the security and credibility of information storage and transmission. Afterwards, based on Hyperledger Fabric, the system architecture of cereal and oil food full supply chain information safety management prototype was designed, thus realizing the functions of its information collection, query, monitoring and traceability. At last, the system was realized based on Browser/Server network structure. Besides, through the verification and analysis of specific application cases, it can provide a new solution and reference for the quality and safety of cereal and oil.

Key words: cereal and oil food; whole supply chain; information security; blockchain; Hyperledger; smart contract

0 引言

近年来,食品安全问题受到了国家和政府的高

度关注^[1-2],这些问题暴露了当前食品安全管理体系中存在的诸多漏洞。粮油是对谷类、豆类等粮食和油料及其加工成品和半成品的统称,是人类赖以

收稿日期: 2019-10-29 修回日期: 2019-12-20
基金项目: 国家重点研发计划项目(2017YFC1600605)和北京工商大学基本科研业务费——青年教师科研能力提升计划项目(PXM2019_014213_000007)
作者简介: 许继平(1979—),男,副教授,博士,主要从事复杂系统建模与实现研究,E-mail: xujiping@139.com
通信作者: 张新(1989—),男,讲师,博士,主要从事检测和物联网技术研究,E-mail: zhangxin@btbu.edu.cn

生存的必需品,其供应链的安全直接影响粮油食品品质的安全,因此粮油食品供应链信息安全监管尤为重要。目前,在对粮油供应链的研究上,各国政府、相关企业构建了供应链信息监管体系,通过将溯源体系纳入法律体系,构建统一的追踪溯源标识码,对供应链上信息进行追踪溯源^[3-12]。然而这并不能完全解决供应链信息安全管理中存在的问题。

粮油食品供应链具有全生命周期长、环节复杂、危害物种类多、信息多源异构等特点,其信息安全管理研究中目前尚未完全解决的问题主要有:一是由于粮油食品供应链参与主体多、环节跨地域、循环周期长,有别于其他食品供应链参与主体,粮食食品供应链各环节参与企业或组织不同,供应链信息共享性差,各环节主体相互之间,尤其是非相邻环节主体之间,存在数据信任问题。二是目前的供应链管理系统大多以参与主体为中心的自建、自主管理为主,在现实层面中主要通过一系列的法律法规、各级政策规范、参与人员的职业道德等进行监管,在与现实层面平行的计算机信息层面中,存在信息丢失和易被篡改的问题。三是在粮油食品全供应链中,目前大都是以静态标识追溯基本信息,而全生命周期多维异构信息的动态实时追溯更加重要。

区块链是一种分布式账簿技术^[13-14],具有全网记录、低成本、高效率、安全可靠等技术特点,采用区块链技术可实现网络信息一体化,使供应链上各企业地位平等,推动信息在供应链中高效、流畅地传递,促进信息公开透明,减少中心化带来的信任问题,同时区块链使供应链上信息交互数字化,通过智能合约技术实现数据的核查、校验,使用数字签名和加密技术,使数据安全高效地传输,提高工作效率,保障信息安全可信。近年来,一些研究将区块链技术与食品和农产品供应链结合起来^[15-19]。利用区块链技术,能够建立粮油食品全供应链上多角色之间的信任问题,建立可靠的互信机制,解决信息不对称问题^[20],为信息安全管理提供真实可信的平台。

本文首先对粮油食品全供应链的运作流程进行

分析,基于区块链构建粮油食品全供应链信息安全管理模型,提出基于粮油食品供应链的双模存储机制和智能合约设计方案;然后,基于粮油食品全供应链信息安全模型设计粮油食品全供应链信息安全管理原型系统架构,并提出原型系统设计方案;最后,结合实际案例对所设计的系统进行验证和分析。

1 粮油食品全供应链信息安全管理模型

1.1 粮油食品供应链分析

在粮油食品全供应链中,参与活动的主体主要是:原材料供应商、生产企业、加工制造企业、分销商、销售商、消费者。这些主体之间并不都是相互关联的,目前大多以粮油加工企业为供应链的核心,其通过整合上游种植户、下游销售部门,并借助研究机构、物流企业、金融机构等优势对物流、商流、信息流、资金流实施供应链管理。这种模式下供应链参与企业众多,节点企业的信息水平参差不齐,不同的标准和不一致的存储格式也使信息无法顺利传递且需求信息具有可变更性和时效性。供应链节点是独立的利益体,只专注于各自领域的数据和业务处理,由于缺乏相应的接口标准和规范,它们之间没有信息共享和业务集成,形成了“信息孤岛”。供应链中的信息孤岛不仅影响整个供应链的企业信息建设和信息共享,而且严重影响对供应链的信息监管和追溯。

粮油食品全供应链流程如图 1 所示。粮油食品全供应链上包括种植、仓储、加工、物流和销售等环节。信息安全管理系统需要将供应链所有节点的数据信息都记录在数据库中,其数据信息主要包括作物的基本属性、作物的品质信息、各环节的环境信息、作物加工的流程和操作参数、各环节的管理信息等。为实现粮油食品全供应链信息安全管理系统,需要通过物联网技术采集供应链各环节的数据信息。

1.2 粮油食品全供应链信息安全管理模型

针对粮油食品全供应链的信息安全管理,结合

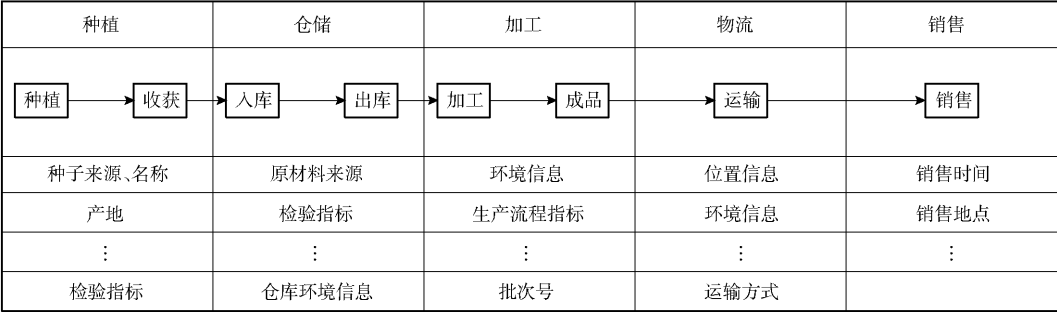


图 1 粮油食品全供应链流程

Fig. 1 Processes of cereal and oil food supply chain

区块链技术,建立与粮油食品全供应链环节对应的区块链节点,采用区块链链式存储和关系型数据库

双模存储机制,构建粮油食品全供应链信息安全管理模型,如图 2 所示。

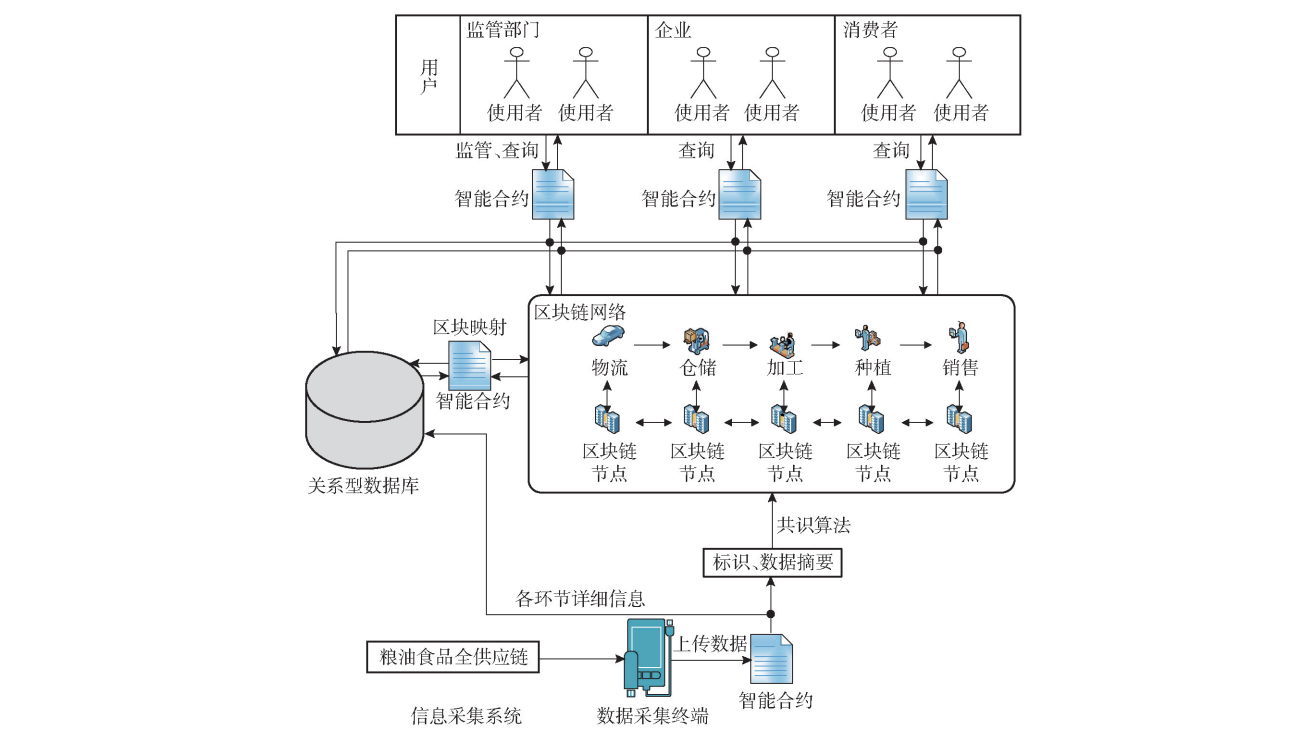


图 2 粮油食品全供应链信息安全管理模型

Fig. 2 Information security management model of cereal and oil food supply chain

整个粮油食品全供应链信息安全管理模型分为 3 部分,包括:粮油食品全供应链信息采集系统、数据管理网络、应用平台。粮油食品供应链上各节点都包含大量的数据,这些数据通过数据采集终端(包括计算机、手机、各类物联网设备等)采集并经过一定的处理后,上传至数据管理网络中。数据管理网络采用的是区块链和关系型数据库构成的双模存储机制,将信息采集系统处理过的数据,通过调用部署在区块链网络上的智能合约校验,在区块链网络中对数据进行广播,使各节点对上传的数据达成共识,然后将信息经过哈希算法转换生成的数据摘要打包成区块保存到区块链网络上的分布式账本中,同时供应链的完整数据信息和智能合约返回的区块和数据间的映射关系,如区块的高度、交易 ID 等,都将保存到链下关系型数据库中。应用平台是基于粮油食品全供应链信息采集系统和数据管理网络的综合应用,其主要服务于粮油食品供应链各环节的相关企业、监管部门和消费者。这些用户通过使用平台提供的相应功能模块执行相应的功能,比如监管部门对供应链进行实时监控、消费者对产品进行溯源查询、企业对自己的信息进行管理和分享等。

数据信息通过数据采集终端获取,经由智能合约验证后形成数据摘要,同时将完整数据上传

到关系型数据库中存储。数据的防篡改机制除了依靠区块链网络自身具有的不可篡改的特点外,还通过智能合约监控区块链网络库和关系型数据库间的映射关系,防止信息发生篡改。粮油食品全供应链信息安全主要面向各相关企业、消费者、监管部门,因此利用区块链赋予各角色不同的权限,通过智能合约依照权限查询或提交相应的信息,既保证了信息的公开透明,又保证了各企业的商业隐私。

1.2.1 “链上+链下”双模存储机制

粮油食品供应链具有节点多、供应链长和涉及面广的特点,链上各环节都包含大量的数据,如果一次性上传到区块链网络中,上传速度慢,区块链的负荷大,运行成本高,而且对区块链网络中每个节点的硬件设施要求都会很高,在本文的模型中,提出一种“链上(on-chain)+链下(off-chain)”双模存储机制,通过将粮油食品供应链上各环节的详细数据信息经过智能合约验证,最终与数据所在的区块链位置信息一同存入关系型数据库中。区块链网络中存储的数据为经过哈希计算的数据以及该数据对应的唯一标识码。通过这种方式,既提高了区块链的运行效率,同时保障数据的安全可信。针对粮油食品全供应链各环节的信息安全管理和追溯,构建了粮油食品全供应链数据存储模型,如图 3 所示。

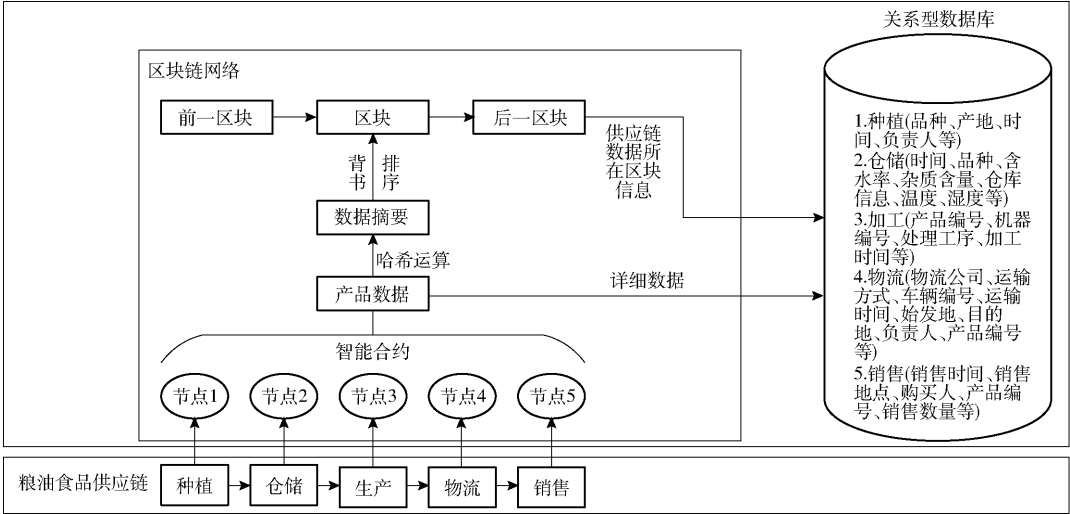


图3 粮油食品全供应链数据存储模型

Fig.3 Data storage model of cereal and oil food supply chain

1.2.2 粮油食品供应链智能合约

智能合约是一种去中心化的、可自行校验、自动执行核心内容的有约束力的数字化协议,通过设置一些可自动触发的执行条件,为区块链网络中的用户提供信息交互、价值转移等功能^[21]。以Hyperledger Fabric 区块链平台为例,其运作流程如图4所示。当智能合约代码编写完成,通过区块链上的节点将智能合约安装到区块链网络中,然后进行初始化和实例化。当节点上传的信息或者调用的功能满足相应合约的触发条件后,系统将自动调用合约实现相应的功能。通过编写智能合约实现对供应链各个环节产品的智能监控。如果已有现成的物联网系统和接口,可以通过接口连接到区块链网络,一旦数据有异常,就会自动触发报警合约,报警信息会发送到企业或监管部门。这些产品标准可以参考粮油食品行业标准、专家意见等,将相应的标准作为智能合约的一部分,验证相应的合约数据和监控链上的交易信息。如图5所示,根据粮食行业国家标准,在智能合约中预先设置数据准入条件,如小麦杂质质量分数在1.0%以内、含水率在12.5%以内等。若通过此环节的粮油食品供应链数据满足预置的数据准入条件,粮油食品可进入供应链的下一个环节,否则系统会提示警告,同时追踪报警源头方便企业和监管部门及时排查并处理安全隐患,避免质量安全事件的发生。

2 粮油食品全供应链信息安全管理原型系统设计

2.1 系统架构

在本文提出的粮油食品全供应链信息安全管理模型基础上,设计了粮油食品全供应链信息安全管理

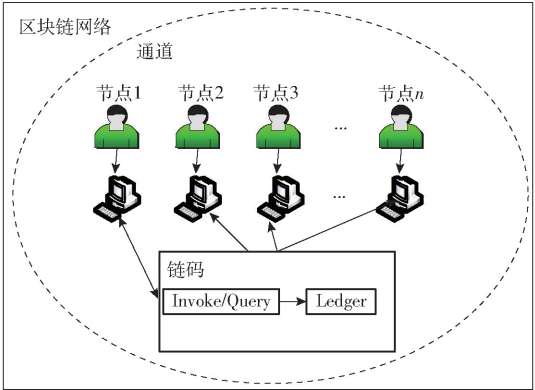


图4 智能合约流程

Fig.4 Processes of smart contract

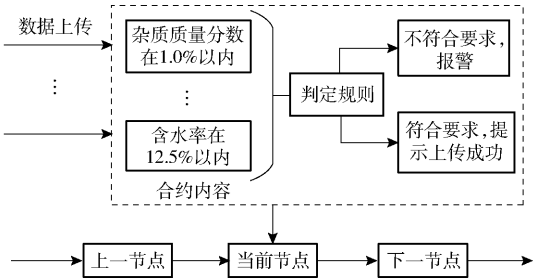


图5 粮油食品供应链智能合约

Fig.5 Smart contract model of cereal and oil food supply chain

理原型系统。系统架构如图6所示,分为物理层、网络层、数据库层和应用层。其中区块链技术主要应用于数据库层和网络层。

物理层主要是数据采集的终端,用于对粮油食品全供应链各环节进行数据采集并使用通信协议上传到系统中。

网络层主要包括网络结构和通信协议。网络主要分为两大类,一类是物联网设备在数据传输时常用的蓝牙、ZigBee、RFID等通信机制;另一类是软件在运行中传输常使用的通信机制,如以太网、WiFi、

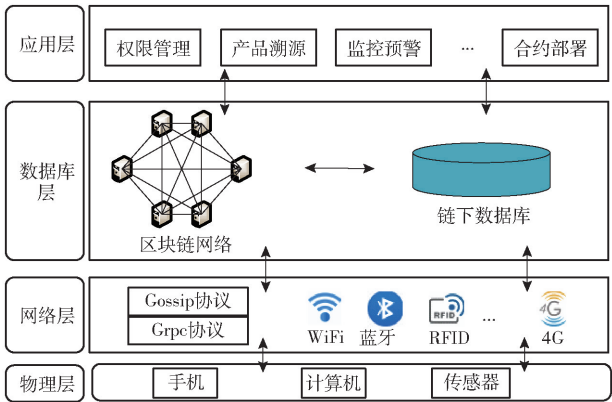


图6 粮油食品全供应链信息安全管理原型系统架构

Fig. 6 Technical framework of information security management prototype system for cereal and oil food supply chain

4G等。本系统通信协议应用的是超级账本平台的数据传输协议,包括Grpc协议和Gossip协议,以提高共识速度和网络安全。

数据库层用来存放系统中所有的数据,由两个部分组成。一部分是区块链网络中的分布式账本,记录了原始数据的数据摘要、时间戳、原始数据的标识码、数字签名等,同时网络中的数据设有访问权限,不同权限的节点查看的信息数量不同;另一部分是链下数据库,主要用来存储通过智能合约验证后的完整原始数据以及其与区块链网络间的映射关系信息。通过这种方法,避免了区块链存储能力不足的问题,同时保证了数据信息的安全可信。

应用层是在已有的区块链网络的基础上,通过底层区块链提供的API接口,设计一个完整的信息安全管理平台,面向的对象主要包括消费者、企业、监管部门和可信的服务提供商,用来实现系统的业务需求。

2.2 系统设计方案

通过对粮油食品全供应链特点的分析,结合供应链上下游企业的实际生产过程,确定了系统的架构。系统主要面向供应链的上下游企业、监管部门和消费者提供服务,包含供应链信息管理、用户管理、质检信息管理、产品溯源和监控预警5个模块,如图7所示。其中,供应链信息管理中包括种植管理、仓储管理、加工管理、物流管理和销售管理5个子模块,主要实现的是粮油食品全供应链生产管理和溯源追踪信息的采集。用户管理为粮油食品全供应链上各环节的不同角色分配不同的功能权限,不同类型的用户相互合作,共同完成粮油食品全供应链信息安全管理系统的运行。质检信息管理提供质检部门的检测信息。监控预警和产品溯源分别为监管部门和消费者提供供应链上的信息。监管部门通

过监控预警模块对供应链上下游企业上传的数据信息以及相关质检单位出具的检验报告进行检查分析,实施对粮油食品全供应链的信息管理。

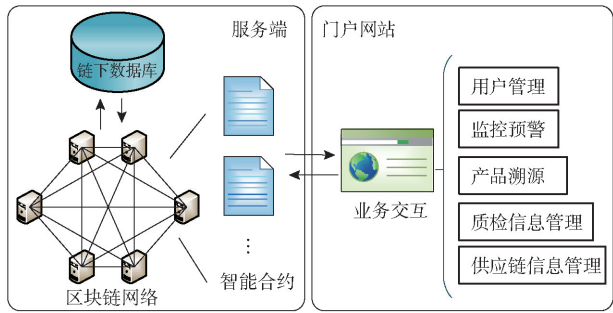


图7 粮油食品全供应链信息安全管理系统

Fig. 7 Information security management system for cereal and oil food supply chain

2.3 系统实现

2.3.1 平台选择

区块链通常被分为公有链、联盟链和私有链。公有链是完全开放的,任何人都可以在公有链上进行交易操作,以比特币、Ethereum(以太坊)等为代表。联盟链是一部分企业或组织组成的,其加入和退出都要经过链上组织的认可,具有部分去中心化的特点,以Hyperledger为代表。私有链一般在公司或组织内部使用,其链上的操作权限都是由一个组织掌握,主要被用来进行内部工作的管理。表1展示了如今两大热门区块链平台的对比分析。通过对比分析,以太坊作为公有链平台,其共识基础为PoW(基于工作量的证明),并不适合应用在供应链这样交易频繁、以信息交互为主的非金融领域。同时Hyperledger作为联盟链平台,在高可用、高性能和隐私保护上优势更明显,其特有的角色权限机制可以使监管部门拥有监管权,也能够对其他角色开放对应的权限,既保护了供应链上的隐私信息,又保证了信息的公开透明。因此本文选择Hyperledger下的Fabric平台来构建粮油食品全供应链信息安全管理系统。

表1 区块链平台对比

Tab.1 Blockchain platform comparison		
特性	Hyperledger Fabric	Ethereum
类别	联盟链	公有链
平台类型	模块化平台	通用平台
开发机构	Linux 基金会	以太坊社区开发者
权限控制	有角色权限分配	无
智能合约	Chaincode(支持 Go,Java 等多语言)	Smart contract code (支持 Solidity 语言)
共识机制	支持多种共识算法	PoW 为主

2.3.2 系统实现过程

软件系统运行于供应链各个环节,功能是记录

当前时刻生产流通情况,读写各环节标识信息,向数据库和区块链网络中发送和接收供应链相关数据,提供查询、追溯、监控等功能。整个系统包含的子系统有粮油食品全供应链区块链系统、粮油食品全供应链信息安全数据库、粮油食品全供应链信息安全管理平台等。系统采用浏览器/服务器(B/S)结构,由数据库、服务器端和用户端组成。

软件平台基于 TCP/IP 协议的网络技术,结合区块链、数据库、软件工程和数据编码等,以 Hyperledger Fabric 作为区块链平台,MySQL 作为云数据库,Go、JavaScript、Html、Css 等作为开发语言构建,使用 Nodejs、Bootstrap 等框架开发,以 Json 格式统一处理和发送数据。系统采用浏览器/服务器(B/S)结构,运行在广域网和局域网中。

(1)数据库

数据库部分采用区块链和关系型数据库结合的设计方法。区块链部分基于 Fabric 开发,区块信息以文件的形式存储在文件系统中,历史数据和区块链的索引存储在默认的 levelDB 数据库中。Fabric 当前支持 levelDB 和 couchDB 两种非关系型数据库,考虑到粮油食品供应链平台调用智能合约产生的业务数据种类多,对于查询的需求较高,因此采用支持富查询的 couchDB 数据库作为 Fabric 的状态数据库。关系型数据库基于 MySQL 开发,在确定需要追溯的数据信息后,建立粮油食品全供应链信息安全数据库,对粮油食品全供应链各环节的信息及区块链网络中的关键信息进行记录。数据库内容由标识码、文字、数字、图像等构成,并根据供应链流程及各环节内部流程作为区分构建独立又相互联系的数据表和库,并通过中心化的信息安全管理平台去采集和检索供应链各环节的信息。

(2)服务器端

区块链平台 Hyperledger Fabric 需要运行在 Linux 环境下。原型系统运行在 VMware 虚拟 PC 软件下的 Ubuntu 操作系统中,Fabric 网络的运行、智能合约的安装、测试和实例化都在 Ubuntu 系统中的 Docker 容器中进行。Fabric 网络采用单机多节点的部署方式,将粮油食品全供应链上的 5 个典型环节和监管部门作为联盟链中的组织,对应 Fabric 中 6 个组织,其中每个组织下包含 2 个 peer 节点,用于实现各组织的背书、记账等功能。同时整个网络还包含 1 个 CA 节点和 1 个 orderer 节点,CA 节点用于管理系统证书的分发验证,orderer 节点用于对数据进行排序服务以生成区块。后端数据服务器主要包含数据处理模块和区块链网络两个部分。数据处理模块基于 nodejs 框架开发,负责接收前端门户网站

传来的表单数据,并统一数据格式,然后通过调用链码将数据上传到区块链网络中,通过验证的数据详细信息会保存到云数据库中,部分公开数据和完整数据的哈希值会经过共识生成区块保存到区块链账本中。区块链网络能够保证供应链信息的真实可信、不可篡改。

Fabric 区块链平台提供了一个强大的角色管理和权限把控机制。通过 Fabric CA 颁发证书,再通过证书生成 Token,最终将 Token 发送给用户,作为各节点用户在网络中的身份凭证。其中证书遵循 X.509 标准,客户端使用 SHA-256 算法对证书进行散列,满足数字签名的参数格式,数字签名采用非对称加密算法 ECDSA 生成的私钥加密,通过核验数字签名的一致性来进行身份认证。当用户需要使用平台进行功能操作时,系统会验证证书的有效性,然后再调用合约对区块链网络进行操作。区块链上各节点对数据信息进行读写操作时,需要相对应的权限去触发不同的合约,当用户权限不够时,只能看到部分公开的数据,无法查看完整数据。

Fabric 区块链平台共识算法采用可插拔设计,目前 Fabric 1.1 版本支持 3 种共识机制,分别是 Solo、Kafka 和 PBFT(实用拜占庭算法)。交易的共识包括 3 个处理阶段:提议阶段、打包阶段和验证阶段。其中 Solo 共识模式是 Fabric 用来进行开发测试的共识算法,只有 orderer 服务节点负责接收交易信息并排序,是最简单的一种排序算法,不适合大规模的实际生产环节;Kafka 共识模式是通过 Kafka 对所有交易信息进行排序,支持对系统中多个 channel 进行单独排序,是一种支持多通道分区的分布式的流式信息处理平台,具有崩溃容错机制,但并不能提供对网络中恶意攻击的保护;PBFT 是基于 BFT(拜占庭算法)改进的分布式容错技术,主要用来解决分布式系统中的信任问题,使区块链网络中的各节点形成对网络状态和数据的共识,PBFT 降低了拜占庭协议运行的复杂度,提高了系统的运行效率,适合对强一致性有要求的区块链应用场景。为了验证模型可信性,简化系统流程,采用 Solo 共识模式构建原型系统的区块链网络。

Hyperledger Fabric 的智能合约又被称为链码(Chaincode)。Chaincode 用来表示系统流程的业务逻辑,它描述了用户的需求,并将其代码化。链码被部署在 Docker 中,Docker 是 Hyperledger Fabric 运行的容器,用于运行区块链网络。一旦链码被部署,它将获得用户可以用来交互的唯一地址,然后通过 Chaincode 客户端可以调用链码,触发它的功能。链码作为一种图灵完备的语言,使用 Go 语言编写。

图 8 所示的例子给出了链码的一些片段,这些代码实现了系统的主要功能。图 8a 展示了种植模块数据采集及查询的智能合约代码。首先进行的是智能合约的初始化过程,然后编写实现种植模块功能的接口代码,包括调用信息上传功能和查询功

```
32 /*初始化方法*/
33 func (c *GrainAndOilChain) Init(stub shim.ChaincodeStubInterface) peer.Response {
34     log.Println("Init GrainAndOilChain start")
35     function, args := stub.GetFunctionAndParameters()
36     if function != "init" {
37         return shim.Error("function is not define")
38     }
39     if len(args) < 1 {
40         return shim.Error("Incorrect number of arguments. Expecting 1")
41     }
42     if args[0] != "init" {
43         return shim.Error("args error")
44     }
45     log.Println("Init GrainAndOilChain success")
46     return shim.Success(nil)
47 }
48 /*执行查询、数据上传方法接口*/
49 func (c *GrainAndOilChain) Invoke(stub shim.ChaincodeStubInterface) peer.Response {
50     log.Println("-----Invoke-----")
51     function, args := stub.GetFunctionAndParameters()
52     log.Println("-----GetFunctionAndParameters-----", function, len(args), args)
53     log.Println(function == "register")
54     log.Println(function == "query")
55
56     if function == "register" {
57         log.Println("-----register-----")
58         return c.register(stub, args)
59     } else if function == "query" {
60         log.Println("-----query-----")
61         return c.query(stub, args)
62     } else {
63         return shim.Error("function not define hahah")
64     }
65     return shim.Success(nil)
66 }
```

(a) 链码的初始化和功能接口

能。图 8b 实现了种植模块的数据上传功能和种植模块的数据信息查询功能。将通过 Web 前端提交的表单信息利用合约代码进行验证,符合要求的会输出“Success”,否则系统会提示数据上传失败。

```
68 /*查询产品信息*/
69 func (c *GrainAndOilChain) query(stub shim.ChaincodeStubInterface, args []string) peer.Response {
70     if len(args) < 1 {
71         return shim.Error("args error")
72     }
73     key := args[0]
74     result, err := stub.GetState(key)
75     if err != nil {
76         log.Println(fmt.Sprintf("query fail key:%s err:%s", key, err))
77         return shim.Error("query fail")
78     }
79     return shim.Success(result)
80 }
81 /*录入产品信息*/
82 func (c *GrainAndOilChain) register(stub shim.ChaincodeStubInterface, args []string) peer.Response {
83     if len(args) != 2 {
84         return shim.Error("args error")
85     }
86     key := args[0] // 品种编号
87     value := args[1] // 产品信息 (用json保存)
88     plant := Plant{}
89     //参数指标判定
90     if ((plant[4]>1)||((plant[5]>12.5){
91         return shim.Error("Substandard Product")
92     }
93     err := json.Unmarshal([]byte(value), &plant)
94     if err != nil {
95         return shim.Error("register fail, parameters cannot be parsed into json objects")
96     }
97     stub.PutState(key, []byte(value))
98     log.Println(key, args)
99     return shim.Success(nil)
100 }
```

(b) 种植模块数据上传和数据查询

图 8 智能合约展示

Fig. 8 Smart contract display

(3) 用户端

Web 前端门户网站是基于当前主流的 TCP/IP 协议,以 JavaScript、Html、Css 等作为开发语言,基于 Bootstrap、jQuery、Ajax 等技术栈开发,并使用 art - template 模板引擎进行渲染的系统对外可视化操作窗口。通过门户网站调用后端服务器提供的 API 接口,实现系统的各项功能,包括用户注册、信息采集、信息查询、实时监控等功能。用户注册通过调用用户注册文件在区块链网络中注册用户信息,区块链网络会赋予用户一个唯一的密钥。用户通过提供密钥验证权限,将门户网站中填写的供应链数据通过表单发送到后端服务器,服务器会对数据进行预处理,统一数据格式。然后,调用链码上传数据到区块链网络中,编码模块会赋予属于一个唯一的 ID,当数据上传成功后,合约会返回数据在区块链网络中的状态信息并存入链下数据库中,完成供应链信息的采集。

3 应用案例分析

通过对山东省某粮食企业下的面粉供应链进行实地调研,该企业下的面粉生产涉及从小麦到面粉销售的完整供应链环节,包含小麦的收购、仓储、加工、运输、销售等流程,收购和仓储环节、加工环节、运输和销售环节分属于不同子工厂,各环节都有比较详细的信息记录,但是各环节之间的信息并不能很好地互联互通,不能形成一条完整的信息链,从而导致信息处理效率低、查询繁琐。经过分析,采用本

研究设计的粮油食品供应链信息安全管理原型系统对其信息管理进行优化。

系统运行界面如图 9 所示。图 9a 为整个系统的用户登录界面,其提供供应链各节点的登录服务和产品溯源服务。系统用户登录后会进入系统的监控界面,如图 9c 所示,从界面中,用户能够监控整个区块链网络的运行区块,包括查看区块信息、链码数量、节点数量等。用户可以通过信息采集功能上传供应链数据信息,系统会自动调用智能合约对数据进行相应的处理,检查数据是否符合条件并赋予其唯一的编码。然后数据信息会保存到区块链网络中,保证数据不可篡改且可追溯。不同环节的信息都会上传到系统中,保存到同一条区块链上,当产品出现问题时,监管部门和企业通过区块链网络和各环节编码能够快速追踪产品信息,及时发现问题源头,并根据产品信息哈希值判断产品真伪和数据信息是否被篡改。图 9c 下方为最新生成区块信息,点击交易细节能够查看区块中的详细信息,如图 9d 所示。通过登录界面上的产品追溯系统,消费者能够利用产品追溯码查询到产品在整个供应链中的信息,提高了产品的市场信任度,有利于企业的发展,如图 9b 所示。

与传统粮油供应链管理系统相比,区块链驱动的粮油食品供应链管理系统具备去中心化的特性,不依赖某个组织和个人,利用共识机制解决了传统粮油供应链管理中的“信任问题”,作为一种不可篡改的分布式记账系统,链上数据具有时间戳且不可



图9 系统工作界面

Fig.9 System working interface

篡改。区块链系统中各节点企业信息上传标准统一,保障了供应链上的数据能够快速交互,打破了传统粮油供应链中的“信息孤岛”,建立了全新的供应链信息管理生态,一定程度上实现了粮油供应链上各利益相关者的协作和校验,实现了资源的有效整合和效益的最大化。

4 结束语

基于区块链建立了粮油食品全供应链信息安全管理原型系统。首先,在分析供应链环节的基础上构建了粮油食品全供应链信息安全管理模型,为改善链式冗余存储的效率问题,设计了区块链和关系型数据库相结合的双模数据存储机制,为实现产业链业务数据交互和全供应链危害物信息监管,设计了定制化部署的粮油食品供应链智能合约;然后,以管理模型为基础,提出了原型系统架构和设计方案,并基于 Hyperledger Fabric 框架,给出原型系统的数据库、服务器端和用户端的具体实现过程;最后,结合具体的应用案例,分析了本原型系统的特点和优势。设计的原型系统能够实现粮油食品全供应链环节信息的共享和互通,并保证信息存储和传输的安全可靠,防止信息孤岛和恶意篡改,为供应链参与主体、消费者、第三方监管部门提供了可信的产业链信息来源,同时为粮油食品供应链危害物风险评估、预测和预警提供了完备的数据基础。

参 考 文 献

[1] 厉曙光,陈莉莉,陈波. 我国 2004—2012 年媒体曝光食品安全事件分析[J]. 中国食品学报,2014,14(3): 1-8.
LI Shuguang, CHEN Lili, CHEN Bo. The analysis of food safety incidents exposed by the media from 2004 to 2012 in China [J]. Chinese Journal of Food Science, 2014,14(3): 1-8. (in Chinese)

[2] 程建. 粮油食品安全存在的问题及对策[J]. 食品安全导刊,2017(36): 11.

[3] 张欣露,王成,吴勇,等. 集成传感器电子标签在农产品溯源体系中的应用[J]. 农业机械学报,2009,40(增刊): 129-133.
ZHANG Xinlu, WANG Cheng, WU Yong, et al. Integration in RFID tags for agricultural traceability[J]. Transactions of the Chinese Society for Agricultural Machinery, 2009,40(Supp.): 129-133. (in Chinese)

[4] MONDAL S, WIJEWARDENA K, KARUPPUSWAMI S, et al. Blockchain inspired RFID based information architecture for food supply chain[J]. IEEE Internet of Things Journal, 2019, 6(3): 5803-5813.

[5] YAN C, HUANHUA F, ABLIKIM B, et al. Traceability information modeling and system implementation in Chinese domestic sheep meat supply chains[J]. Journal of Food Process Engineering, 2018, 41(7): e12864.

[6] KHAN M S, KHAN M M I, HALEEM A, et al. Selection of traceable technology in food supply chain[C]//IOP Conference Series: Materials Science and Engineering. IOP Publishing, 2018: 012010.

[7] 董玉德,丁保勇,张国伟,等. 基于农产品供应链的质量安全可追溯系统[J]. 农业工程学报,2016,32(1): 280-285.
DONG Yude, DING Baoyong, ZHANG Guowei, et al. Quality and safety traceability system based on agricultural product supply chain[J]. Transactions of the CSAE, 2016,32(1): 280-285. (in Chinese)

[8] 杨佳,屠康. 基于物联网技术的稻米产业链质量追溯系统研究[J]. 农产品质量与安全,2018(2): 8-12.

[9] PIGINI D, CONTI M. NFC-based traceability in the food chain[J]. Sustainability, 2017,9(10): 1910.

[10] LIU P, LIU W, LI Q, et al. A research on tracing code of culture of food safety traceability based on RFID and improved EPC [C]//2016 International Conference on Logistics, Informatics and Service Sciences (LISS). IEEE, 2016: 1-6.

[11] ZHANG X, WANG J, CUI J, et al. Design of distributed traceability system for wheat products quality[C]//International Conference on Computer and Computing Technologies in Agriculture. Springer, Berlin, Heidelberg, 2011: 498-507.

[12] ZHANG Y, WANG W, YAN L, et al. Development and evaluation of an intelligent traceability system for waterless live fish

- transportation[J]. Food Control, 2019, 95: 283 – 297
- [13] 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.
YUAN Yong, WANG Feiyue. Blockchain: the state of the art and future trends[J]. Acta Automatica Sinica, 2016, 42(4): 481 – 494. (in Chinese)
- [14] 邵奇峰, 金澈清, 张召, 等. 区块链技术: 架构及进展[J]. 计算机学报, 2018, 41(5): 969 – 988.
SHAO Qifeng, JIN Cheqing, ZHANG Zhao, et al. Blockchain: architecture and research progress[J]. Chinese Journal of Computers, 2018, 41(5): 969 – 988. (in Chinese)
- [15] TIAN F. A supply chain traceability system for food safety based on HACCP, blockchain & Internet of things[C] // 2017 International Conference on Service Systems and Service Management. IEEE, 2017: 17066653.
- [16] TIAN F. An agri-food supply chain traceability system for China based on RFID & blockchain technology[C] // 2016 13th International Conference on Service Systems and Service Management (ICSSSM). IEEE, 2016: 16214816.
- [17] KRZYZANOWSKI K. Putting food on the blockchain: a regulatory overview[J]. Journal of Food Distribution Research, 2019, 50(1): 86.
- [18] 于丽娜, 张国锋, 贾敬敦, 等. 基于区块链技术的现代农产品供应链[J/OL]. 农业机械学报, 2017, 48(增刊): 387 – 393.
YU Li'na, ZHANG Guofeng, JIA Jingdun, et al. Agricultural product supply chain based on block chain technology[J/OL]. Transactions of the Chinese Society for Agricultural Machinery, 2017, 48(Supp.): 387 – 393. http://www.j-csam.org/jcsam/ch/reader/view_abstract.aspx?flag=1&file_no=2017s059&journal_id=jcsam. DOI: 10.6041/j.issn.1000-1298.2017.S0.059. (in Chinese)
- [19] 陶启, 崔晓晖, 赵思明, 等. 基于区块链技术的食品质量安全管理系统及在大米溯源中的应用研究[J]. 中国粮油学报, 2018, 33(12): 102 – 110.
TAO Qi, CUI Xiaohui, ZHAO Siming, et al. The food quality safety management system based on block chain technology and application in rice traceability[J]. Journal of the Chinese Cereals and Oils, 2018, 33(12): 102 – 110. (in Chinese)
- [20] 周清杰, 王艳飞, 傅星. 信息不对称, 区块链与食品安全社会共治[J]. 中国市场监管研究, 2016(11): 53 – 56.
- [21] 欧阳丽炜, 王帅, 袁勇, 等. 智能合约: 架构及进展[J]. 自动化学报, 2019, 45(3): 445 – 457.
OUYANG Liwei, WANG Shuai, YUAN Yong, et al. Smart contracts: architecture and research progresses[J]. Acta Automatica Sinica, 2019, 45(3): 445 – 457. (in Chinese)
-

(上接第 340 页)

- [22] CHONG C Y, KUMAR S P. Sensor networks: evolution opportunities and challenges[J]. Proc. of the IEEE, 2003, 91(8): 1247 – 1256.
- [23] ZHANG Z. Investigation of wireless sensor networks for precision agriculture[R]. American Society of Agricultural and Biological Engineers; 2004 ASAE Annual Meeting, 2004, Paper Number: 041154.
- [24] 吕恩利, 陆华忠, 王广海, 等. 一种畜禽养殖环境参数多点无线智能监控系统及其方法; 201910281334.3[P]. 2019-04-09.
- [25] NJEKWA K S. A cost efficient wireless sensor network for grain storage and environmental monitoring based on ZigBee and Arduino[D]. Guangzhou: South China University of Technology, 2018.
- [26] WANG J, LIU Y, LI M, et al. QoF: towards comprehensive path quality measurement in wireless sensor networks[C] // IEEE INFOCOM 2011. Shanghai: IEEE, 2011: 10 – 15.
- [27] ZHOU Y, WEI M, HAO Z. Research on ZigBee indoor technology positioning based on RSSI[J]. Procedia Computer Science, 2019, 154: 424 – 429.
- [28] 何延杰, 李腊元, 邢明彦. WSN 中一种能量均衡的分簇路由协议的设计[J]. 传感器技术学报, 2009, 22(10): 1510 – 1514.
HE Yanjie, LI Layuan, XING Mingyan. Design of an energy balanced cluster-based routing protocol for WSN[J]. Chinese Journal of Sensors and Actuators, 2009, 22(10): 1510 – 1514. (in Chinese)
- [29] 吕恩利, 陆华忠, 王广海, 等. 一种环境多源信息感知和预警系统及其方法; 201910281348.5[P]. 2019-04-09.
- [30] BJARNE K, 马晓迪. 分娩舍的规格和设计[J]. 国外畜牧学(猪与禽), 2012, 32(3): 9 – 11.