doi:10.6041/j.issn.1000-1298.2021.05.022

区块链驱动的稻米供应链信息监管模型研究

许继平[1,2]　王　健[1,2]　张　新[1,2]　王小艺[1,2]　孔建磊[1,2]　刘　阳[3]

(1.北京工商大学中国轻工业工业互联网与大数据重点实验室,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;
3.中国信息通信研究院,北京 100191)

摘要:针对稻米供应链业务主体复杂、信息流转冗长、数据利用率低、监管覆盖性差等问题,构建了区块链驱动的稻米供应链信息监管模型,并进行系统化实现。首先,对稻米供应链信息流转特性进行分析,梳理并提炼供应链各业务环节主体及关键信息;然后,以区块链驱动构建稻米供应链信息监管模型,设计隐私数据分级加密存储模式和定制化业务逻辑监管智能合约;最后,基于 Hyperledger Fabric 开源框架,构建并实现稻米供应链信息监管原型系统,并以湖南省常德市某粮油企业为例,进行了应用案例实证分析。结果表明,构建的稻米供应链信息监管模型及原型系统能够解决稻米供应链数据隐私加密、安全存储及权限管理等问题,实现供应链信息互联互通和有效监管。本研究可为粮油质量安全监管提供一种可行的应用方法。

关键词:稻米供应链;信息监管;区块链;隐私加密;智能合约;超级账本

中图分类号:S126;TP309.2　　**文献标识码**:A　　**文章编号**:1000-1298(2021)05-0202-10　　**OSID**:

Information Supervision Modeling of Rice Supply Chain Driven by Blockchain

XU Jiping[1,2]　WANG Jian[1,2]　ZHANG Xin[1,2]　WANG Xiaoyi[1,2]　KONG Jianlei[1,2]　LIU Yang[3]

(1. *Key Laboratory of Industrial Internet and Big Data (Beijing Technology and Business University), China National Light Industry, Beijing* 100048, *China*
2. *Beijing Key Laboratory of Big Data Technology for Food Safety, Beijing Technology and Business University, Bejing* 100048, *China*
3. *The China Academy of Information and Communications Technology, Bejing* 100191, *China*)

Abstract: Aiming at the problems of complex business entities, long information flow, low data utilization and low regulatory coverage in rice supply chain, a information supervision model of rice supply chain driven by blockchain was built and implemented systematically. Firstly, the information flow characteristics of rice supply chain were analyzed, and the main body and key information of each business link in the supply chain were sorted out and refined. On this basis, the supervision model of rice supply chain information driven by blockchain was constructed, the hierarchical encryption storage mode of private data and the customized business logic supervision intelligent contract were designed. Finally, based on the Hyperledger Fabric open source framework, the rice supply chain information supervision prototype system was constructed and implemented. In addition, taking a grain and oil enterprise in Changde City of Hunan Province as an example, the application case analysis was carried out. The results showed that the rice supply chain information supervision model and prototype system constructed can solve the problems of rice supply chain data privacy encryption, secure storage and authority management, realize supply chain information interconnection and effective supervision, which can provide a way for grain and oil quality safety supervision feasible and practical application solutions.

Key words: rice supply chain; information supervision; blockchain; privacy encryption; smart contract; hyperledger

收稿日期:2021-01-24　修回日期:2021-02-24

基金项目:国家重点研发计划项目(2019YFC1605306、2017YFC1600605)和国家自然科学基金项目(62006008)

作者简介:许继平(1979—),男,副教授,博士,主要从事区块链和智能信息处理研究,E-mail:xujiping@139.com

通信作者:张新(1989—),男,副教授,博士,主要从事区块链和 AI 融合应用研究,E-mail:zhangxin@btbu.edu.cn

0　引言

稻米是中国主要粮食作物之一，全国近 2/3 人口以稻米作为主食[1]，稻米的质量安全直接关系到人民健康与国家稳定。近年来，各种稻米质量安全问题时有发生，如镉大米[2-3]、香精米、陈化粮等事件，因此亟需进行高效的稻米供应链信息监管。

稻米不同于其他食品，其供应网络复杂、循环流通周期长，且各环节风险因素与危害物种类多、分布环节广、差异大[4-5]。此外，稻米供应链各环节相对独立，相互之间信息交流少，各节点难以形成共识。传统的监管系统各环节存在不诚信企业篡改检测数据等问题，从而降低了监管结果的可信度[6]。并且传统供应链监管模式在进行监管时，需要对供应链各环节数据进行大量的重复验证和检查工作，导致时间成本较高、信息流转冗长，从而使监管工作效率低下[7-8]。

区块链技术具有通过信任机制根据业务规则自动执行约定代码的特性，能够将全流程数据清晰地记录到链上，进而真实可靠地传递资金流、物流和信息流[9-11]。近些年，国内外研究人员在区块链结合食品供应链监督与管理方面进行了研究探索，通过各种标识技术建立产品标识[12-13]，应用传感器在供应链流通环节进行检测[14]，并制定相应管理体系[15]，建立对食品进行数据上传、实时监控、风险预警和信息溯源的供应链管理系统[16]。研究发现，区块链技术能够有效提高食品供应链数据的安全性与信息可追溯性，为食品质量安全监管提供了有力保障。但是，由于稻米供应链各环节关键数据信息繁杂，各企业主体不能形成统一标准，并且区块链网络内各节点并非完全匿名，其隐私保护存在风险，因此对于上链数据进行隐私加密非常必要[17-19]。此外，目前稻米供应链监管采用的智能合约流程普遍较短，且各合约分工不明确，不能贯穿全监管流程，难以有效发挥合约功能[20]。因此，构建适用于稻米供应链的信息监管机制具有重要的现实意义和应用价值。

本文对稻米供应链业务流程及流转特性进行全方位分析，梳理并提炼供应链各业务环节主体及关键信息；结合区块链技术构建稻米供应链信息监管模型，提出隐私数据分级加密及存储模式和定制化业务逻辑监管智能合约；设计稻米供应链信息监管原型系统，并以某粮油企业为例进行分析验证。

1　关键技术

区块链最初被定义为一种将数据区块按时间顺序相连而成的一种分布式账本[21]。而随着研究深入，对于区块链技术的认知逐渐在发生变化[22-23]，当前研究认为区块链指利用块链式数据结构来验证和存储数据，并采用分布式节点共识算法生成和更新数据，同时应用密码学原理来确保数据传输与信息存储安全，此外还以智能合约进行数据操作的一种分布式架构与计算范式，其去中心化、不可篡改、可追溯与自洽性的特性，符合供应链监管系统对于确保信息安全隐私与高可追溯性等需求。本文以区块链技术为驱动，构建稻米供应链信息监管模型，并基于区块链开源框架超级账本平台实现原型系统。

密码学是区块链隐私安全保障的核心，区块链中主要涉及的密码学算法主要包括非对称加密算法、默克尔树和哈希算法。在本文中建立隐私数据分级加密及存储模式部分采用了哈希算法中 SM3 密码杂凑算法与对称加密算法中高级加密标准加密算法（Advanced encryption standard，AES）。密码杂凑算法可以将任意长度数据压缩为固定长度信息摘要，用于数字 a 签名和数据完整性保护[24]。AES 加密用于保证数据的机密，其通信双方在加密和解密过程中采用相同的密钥[25]。AES 算法分为多种加密模式，在本文中模型构建时便结合了加密反馈模式（Cipher feedback，CFB）与电子密码本模式（Electronic codebook，ECB）。

智能合约具有自行校验、去中心化和自动执行等特点[17,26-28]，并能够自行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与价值转移等功能，本文中监管模型需要通过智能合约来实现相应业务逻辑。

2　稻米供应链业务主体及信息流转分析

稻米供应链各环节参与企业主体众多，包括种植者、收购商、仓储企业、加工企业、物流企业与分销商等，其中稻米供应链生命周期长、环节复杂，链上各企业主体普遍存在数据标准差异化与存储格式不一致的问题。同时，目前市场缺乏统一稻米供应链监督与管理系统，导致不相邻企业主体之间关联性较小，信息流通差、流转冗长，部分关键数据的隐私安全得不到保障，存在丢失或被篡改的风险，不利于供应链节点信息溯源和相关部门监管。此外，由于稻米供应链循环流通周期较长且各环节之间信息不对称，监管者难以确定到达消费者手中的问题稻米是在哪一供应链主体环节造成的，并且出现问题不易补救，亟需构建安全高效的监督和管理体系。

针对上述问题，将稻米供应链流程从信息监管角度分为上、中、下 3 个阶段，如图 1 所示。供应链上游包括种植环节；中游包括收储、加工、仓储和运

输环节,其中收储中又包含收购、干燥、除杂和入仓环节,加工包括垄谷、碾米、色选、抛光和包装环节;下游为销售环节。销售商将稻米最终售卖给消费者,监管者则对于供应链进行监督管理。其中加工环节是稻米供应链核心环节,既能指导限制上游稻米收储与种植环节,又可以为下游销售环节提供生产资料,并借助物流企业、仓储企业和金融机构等对物流、商流、信息流和资金流进行统一分配与管理,因而对粮油加工企业加强监管十分必要。在稻米供应链信息监管的过程中,各企业都有一些信息是敏感的,无法完全公开,如交易记录、成本信息和危害物信息等,因此需要对上传到区块链上的信息进行分类,以区分敏感度和优先级,保证高效监管的同时保护信息不被泄露。

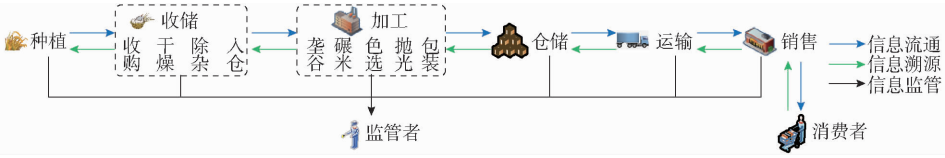


图 1 稻米供应链流程图

Fig. 1 Flowchart of rice supply chain

根据稻米供应链流程及供应链上各企业主体业务特点,本文将稻米供应链 13 个环节关键数据信息分为 5 类,分别为主体信息、基本信息、危害物信息、环境监测信息和交易记录与价格信息,如表 1 所示。表内所提取信息分类皆是各环节关键信息摘要,以加工环节为例,加工企业接收来自于仓储企业在内的多个粮仓存储的稻米。稻米运送到加工厂后,加工厂对产品进行垄谷、碾米、色选、抛光和包装等流程。根据文献查阅及网络资源调研,稻米中重金属危害物除了受产地环境因素的影响外,对其影响最大的过程就是稻米加工环节,在这个环节受机器加工的影响,重金属含量有明显的增加。因此,在本环节所需要记录的信息除了包括企业信息、环境监测信息、垄谷方式、出糙率、脱壳率、碾米方式、整米率、碎米率、色选精度、抛光率、产品包装编号和产品批次号等,还包括不同子环节的真菌毒素和重金属含量。详细信息分类能够进一步优化供应链业务体系流程架构,并可作为稻米质量安全全链条信息监管模型建立的基础。

3 模型构建

完整的监管模型不仅需要政府机构对供应链的监管,还需涵盖供应链各企业主体数据上传、查询和消费者商品溯源部分,实现监管一体化。这样一方面可以从供应链对稻米信息进行监督管理,确保稻米供应链数据流通时信息安全性与真实性,另一方面也使得供应链企业主体之间、监管机构与供应链各企业主体之间减少信息差,避免产生信息孤岛。本文根据稻米供应链流程特点与链上各企业主体业务逻辑,结合区块链技术、密码学与智能合约构建了稻米供应链信息监管模型,如图 2 所示。

本文将稻米供应链上各环节都视为区块链网络中的一个节点,每个节点都对应一个云数据库。供应链上各节点通过业务系统调用部署在区块链网络中的智能合约,经过共识后,大部分数据明文与密文记录到云数据库中,小部分数据明文、信息摘要与密钥保存到区块链网络中。稻米供应链企业主体节点由种植企业(种植户)为起始,由供应链流通方向至销售企业,最终稻米售卖到消费者手中。流通过程中供应链各企业主体将采集数据通过合约上传至区块链网络与云数据库。监管部门会向区块链网络发起请求调用对应合约验证权限,实现对供应链进行实时监管。供应链各企业主体与消费者也可以采取不同方式对区块链网络发起同样信息查询溯源请求,在权限范围内查询产品信息,以验证稻米是否符合应达标准或信息是否遭到篡改。

3.1 隐私数据分级加密及存储模式

由于区块链网络内各节点并非完全匿名,因此其隐私保护存在安全性风险。虽然区块链数据传输并未直接与真实世界的企业身份相关联,但区块链中数据是完全公开透明的。随着各种反匿名甄别技术的发展,对一些关键目标的信息破解与定位识别逐步出现,因此对于上链数据进行隐私加密十分关键。本文结合链上链下双模存储设立了隐私数据分级加密及存储模式,将数据根据其隐私程度进行分级,并综合考虑安全性与加密效率,根据隐私级别与数据量采用不同的加密方式对统一格式的数据进行加密并上传至区块链网络与云数据库,如图 3 所示。

该模式基于稻米供应链各环节关键信息分类,并综合稻米供应链各环节不同数据隐私程度、加密算法安全性与算法时间复杂度和空间复杂度,对供应链流通数据进行分级加密及安全存储,具体内容包含以下 3 点:

(1)交易记录与价格信息定义为一级隐私数据。对于一级隐私数据,本模式采用 AES 算法 CFB 模式进行加密后将数据密文传入云数据库,CFB 模

表 1　稻米供应链各环节关键信息分类

Tab.1　Classification of key information in rice supply chain

稻米供应链环节		关键数据信息分类				
		主体信息	基本信息	危害物信息	环境监测信息	交易记录与价格信息
种植		种植户身份信息；种植许可证信息；联系方式；营业执照信息（可无）	种子来源；稻米种类；产地信息；种植时间；收获时间；肥料信息及使用记录；农药信息及使用记录	真菌毒素：黄曲霉毒素 B1、赭曲霉毒素 A、脱氧雪腐镰刀菌烯醇 重金属：铅（Pb）、镉（Cd）、总汞（Hg）、无机砷（As）、铬（Cr） 农药残留：毒死蜱、三唑磷、丁硫克百威、苄嘧磺隆、乙草胺、丁草胺、苄磺隆等 病虫害：稻黑色菌核秆腐病、稻白叶枯病、稻矮缩病等	稻米各生长周期图像；环境实时温度；环境实时湿度；环境实时光照强度；土壤水分含量；环境氧气/二氧化碳浓度	种子价格；肥料价格；总成本；销售价格；收储企业信息
收储	收购	企业名称；企业地址；企业法人信息；相关环节负责人信息；许可证信息；企业联系方式	收购时农药抽检记录	真菌毒素：黄曲霉毒素、赭曲霉毒素 A、玉米赤霉烯酮、脱氧雪腐镰刀菌烯醇；熏蒸剂及除虫剂残留：溴甲烷、磷化氢和磷化铝等	无	种植户信息；收购价格；干燥、除杂、仓储等成本；销售价格；加工企业信息
	干燥		干燥方式（自然/机械）；干燥前含水率；干燥后含水率		环境实时温度；环境实时湿度	
	除杂		含杂量；除杂率			
	入仓		库存编号；产品来源；产品数量；入库时间；质检编号；出库时间		环境温度、湿度、氧气浓度、二氧化碳浓度、甲醛、TVOC	
加工	垄谷	企业名称；企业地址；企业法人信息；相关环节负责人信息；许可证信息；企业联系方式	垄谷方式（垄谷机品牌）；出糙率；脱壳率	真菌毒素：黄曲霉毒素；熏蒸剂残留物 重金属：铅（Pb）、镉（Cd）、总汞（Hg）、无机砷（As）、铬（Cr）	环境实时温度；环境实时湿度	加工成本；加工价格
	碾米		碾米方式（化学法/机械法）；整米率；碎米率			
	色选		色选精度；带出比			
	抛光		抛光率			
	包装		产品包装编号；产品批次号；产品质量信息			
仓储		仓储企业名称；仓储企业地址；企业法人信息；仓储管理员信息；许可证信息；管理员联系方式	库存编号；产品来源；产品数量；入库时间；质检编号；出库时间	真菌毒素：黄曲霉毒素、赭曲霉毒素、脱氧雪腐镰刀菌烯醇	环境温度、湿度、氧气浓度、二氧化碳浓度、甲醛、TVOC	仓储成本；仓储价格
运输		物流企业名称；物流公司地址；运输负责人信息；许可证信息；负责人联系方式	运输工具；工具编号（车牌号）；出发地；出发时间；目的地；抵达时间	温湿度异变霉生成的真菌与毒素，如黄曲霉毒素等	车内环境温度；车内环境湿度；车内氧气/二氧化碳浓度	物流成本；物流价格
销售		商家名称；商铺地址；商铺负责人信息；营业许可证信息；商家联系方式	产品名称；产品数量；进货时间；进货编号；出货时间	无	销售环境照片	收购价格；销售价格

式能够加密任意长度的明文，以适应稻米供应链各节点用户不同数据格式需求。此外，数据密钥由算法随机生成，并将其上传至区块链网络进行存储，能够极大确保密钥的随机性与安全性，解决了对称加密存在的密钥泄露风险。

（2）危害物信息定义为二级隐私数据。本模式则采用 AES 算法 ECB 模式对二级隐私数据进行加密后传入云数据库。相较于 CFB 模式，ECB 模式较为简单，并且能够进行大量的并行计算，适合数据量较大的稻米危害物信息。在这一过程中数据密钥生

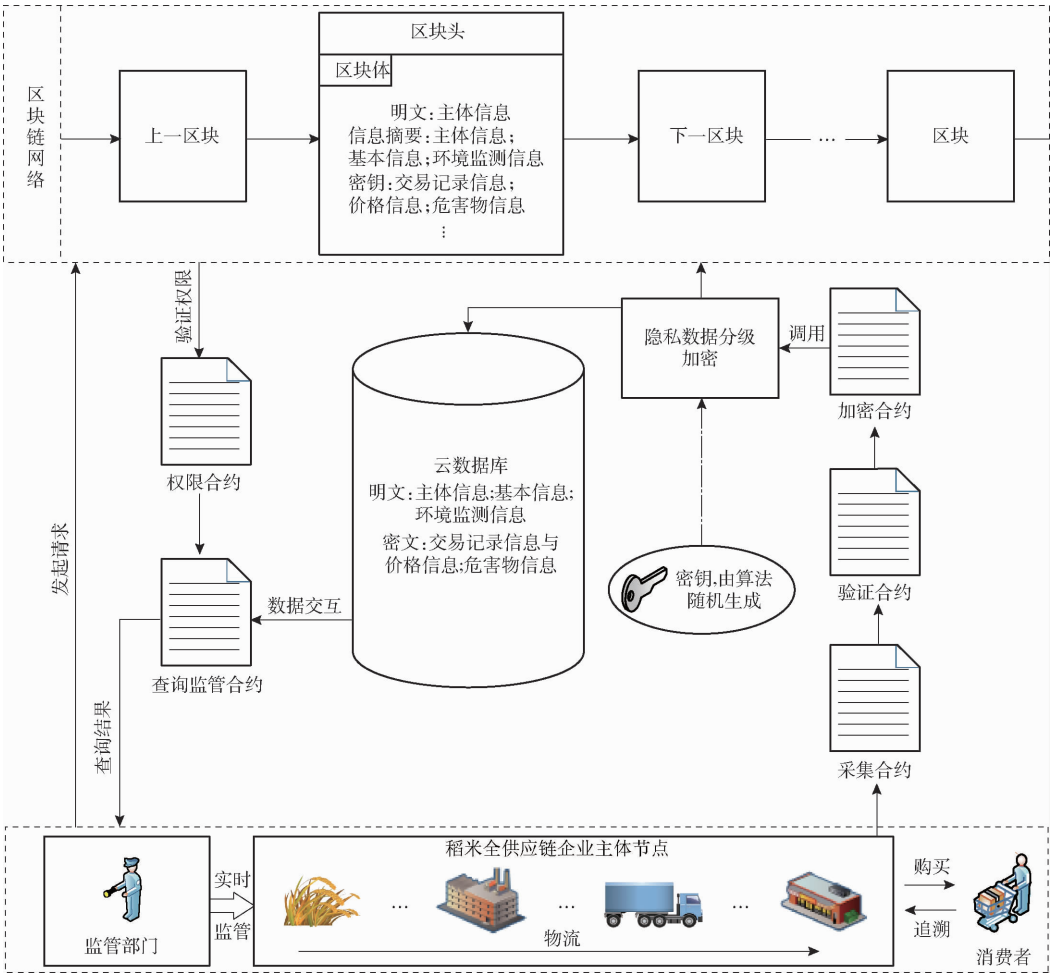


图 2 稻米供应链信息监管模型

Fig. 2 Information supervision model of rice supply chain

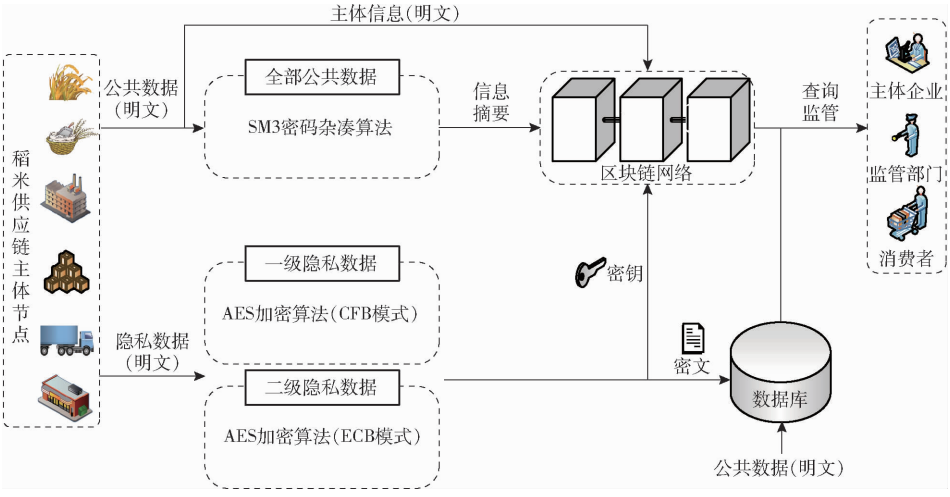


图 3 隐私数据分级加密及存储模式

Fig. 3 Classified encryption and storage mode of privacy data

成与存储的方式与一级隐私数据相同。

(3)主体信息、基本信息和环境监测信息定义为公共数据。其中对于主体信息,其数据量少且重要程度高,本模式采用直接将数据传输至区块链网络的方式;而对于全部公共数据则采用 SM3 密码杂凑算法进行加密,然后将加密生成的信息摘要上传至区块链网络,公共数据明文上传至云数据库。

该模式通过采用多种加密算法对数据进行分级加密的方式,在利用最少计算资源的前提下,将稻米供应链数据分散化存储,确保了上传至区块链网络与云数据库中的数据在流通与存储过程中的安全与隐私。

3.2 多业务逻辑监管智能合约

智能合约是区块链结合稻米供应链信息监管模

型中的关键部分，整个模型都需要通过智能合约来实现相应业务逻辑。通过编写具有自行校验功能的智能合约能够有效弥补传统监管需进行大量重复验证检查工作、时间长和效率低的问题。本文中采用层级化智能合约对整个模型的多个业务逻辑流程进行梳理与构建，这样能够进一步划分各个合约的职能，令模型的逻辑流程更为清晰，并为后续系统模型的进一步优化提供了便利条件。

如图 4 所示，本文中应用合约的业务逻辑流程分为 2 部分：数据上传与数据查询（监管）。数据上传即稻米供应链主体将企业数据传输至监管系统，包括对数据的采集、验证与加密；数据查询即监管部门、主体企业和消费者对链上链下数据进行数据的溯源查询，不同节点的主体具有不同的权限。

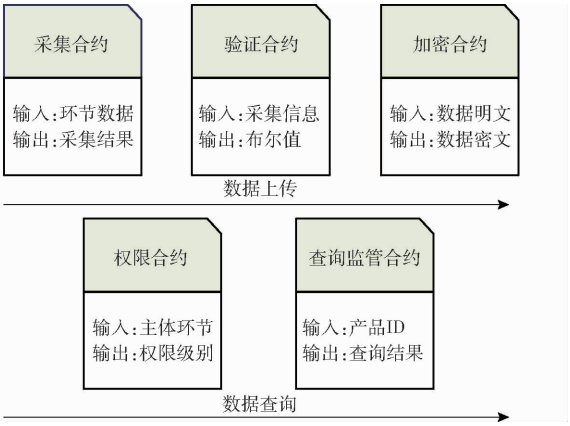


图 4　模型合约逻辑流程

Fig. 4　Contract logic flow of model

3.2.1　数据采集

稻米供应链某环节企业主体数据采集合约算法为：

```
Input: m 份环节数据
Output: return 数据采集结果
for t in range(m):
  if 用户拥有上传权限:
    采集信息:{ 参与环节,主体信息,基本信息,危害物信息,环境监测信息,交易记录与价格信息}
    if 通过信息验证:
      调用数据加密上传模块
      return"数据采集成功"
  return "数据不符合规定指标"
```

遍历所有要采集的数据，然后验证用户是否拥有数据上传权限；验证通过后，若检测数据数值在规定范围内，通过物联网设备和应用平台将加密并且格式化后的数据上传至监控系统，合约结束；若过程中出现问题，则返回异常数据信息后合约结束。

采集合约是供应链主体数据上传过程中的核心内容，验证合约与加密合约皆在数据采集算法中被调用，其合约内容为整个模型逻辑构建奠定了基础。

3.2.2　数据验证

验证合约主要是检验采集数据是否满足相关法律法规与规范标准限定的范围，当满足不同的条件时合约将触发不同的功能。以稻米供应链加工环节为例，编写合约时需要根据通用检测指标，重金属含量如铅、镉、汞，真菌毒素含量如黄曲霉素等，并将编写好的验证合约部署至区块链网络中。

验证合约算法为：

```
Input:稻米采集信息
Output: return false/true
if 重金属含量验证:
  Pb < = 0.2 and G < = 0.2 and Hg < = 0.2
  向企业主体和监管部门发送事件报告
  return false
else if 真菌毒素含量验证:
  AFTB1 < = 10
  向企业主体和监管部门发送事件报告
  return false
return true
```

其作用为：当有信息上传时，节点会调用合约对上传的数据进行处理，将上传数据同信息库中的指标进行对比，如果质量指标不满足预置的数据准入条件，系统会执行预置的响应规则，上传数据信息并给企业主体与监管部门发送不良事件报告，如果质量指标符合预置的数据准入条件，系统则会允许其上传。通过验证合约实时监管稻米质量全链条采集信息，方便企业和监管部门及时发现并处理安全隐患，可以有效避免存在质量问题的稻米在供应链上流通。

3.2.3　数据加密

上文分级加密隐私模型内容合约化后即为数据加密算法，输入的参数为统一格式后的数据明文，合约会根据不同的采集数据采取不同的加密方式，将不同格式的密文密钥等传入区块链或数据库，算法为：

```
Input:数据明文
Output: 数据密文(密钥)
全部数据格式化
if 公共数据
  if 主体信息:
    调用区块链网络信息上传模块
  else:
```

SM3 密码杂凑算法加密,生成信息摘要
调用区块链网络信息上传模块(信息摘要)
调用数据库信息上传模块(明文)
else if 隐私数据
if 一级隐私数据:
AES 加密算法(CFB 模式),生成密文与密钥
调用区块链网络信息上传模块(密钥)
调用数据库信息上传模块(密文)
else if 二级隐私数据:
AES 加密算法(ECB 模式),生成密文与密钥
调用区块链网络信息上传模块(密钥)
调用数据库信息上传模块(密文)

数据加密合约即隐私数据分级加密模式的合约化实现,通过智能合约自动执行已封装好的加密逻辑,完成稻米供应链隐私数据分级加密与上传功能,保证供应链信息流通安全的同时提升数据传输效率。

3.2.4 权限管理

权限管理算法是供应链监管与信息查询的重要组成部分,合约以分发不同密钥的方式限制节点权限,算法为:

Input:主体环节
Output: 权限级别
if 企业节点:
调用可查询公开数据模块
if 相邻企业节点:
获取查询节点对应 ECB 密钥
调用数据查询模块
else if 监管节点:
获取监管节点对应 CFB 密钥与 ECB 密钥
调用数据监管模块
else if 消费者节点:
调用可查询公开数据

企业节点能够查询供应链所有公开数据并可获得相邻企业节点的对称加密密钥,以查询相邻企业节点二级隐私数据(危害物信息);监管节点有权限获得全部密钥,以对供应链进行监管;消费者能够消费后扫描商品二维码默认为消费者节点,可以查询所购稻米供应链公开数据。

3.2.5 数据监管查询

针对稻米供应链数据查询,其合约流程算法为:

Input:企业信息/参与环节/产品 ID
Output: return 查询结果
if 用户拥有查询权限:
调用信息查询模块
if SM3 算法对数据进行运算结果 ! = 链上存储信息摘要:
return"公共数据被篡改"
return 查询信息

节点用户在系统平台上输入要查询的稻米供应链相关信息,验证用户拥有查询权限后系统同时将云数据库与区块链网络数据下载至本地,并采用哈希算法对数据库中所下载数据进行信息摘要计算,得到结果与区块链中所存摘要进行比对,若相等则证明数据库中数据未被篡改,返回查询信息,合约结束;若值不等,证明公共数据遭到篡改,则返回错误信息,合约结束。

监管查询合约是监管系统模型数据查询流程的最后一步,返回查询数据同时能够验证数据库中所存储公共数据是否遭到篡改,为数据安全存储设置了双重保障。

4 稻米供应链信息监管系统化实现

4.1 系统架构

基于稻米供应链信息监管模型,设计了稻米供应链信息监管原型系统。该系统架构如图 5 所示,分为应用服务层、数据存储层、业务逻辑层和感知采集层。

应用服务层以网页和手机 APP 的形式向监管部门、企业和消费者用户提供相应功能,并根据用户的不同划分权限级别。

数据存储层包括云数据库与 Hyperledger Fabric 区块链平台存储部分,其中区块链中数据采用文件形式存储。企业将经过系统加密后的数据分别存储在区块链与云数据库,在方便数据查询的同时令数据存储去中心化,防止篡改。

业务逻辑层是以智能合约为核心,确保系统高效运转的同时调用分级隐私加密机制,从而保证存储数据隐私安全。

感知采集层作为数据终端,主要用于收集稻米供应链企业主体全生命周期的各项业务数据和危害物信息。

4.2 系统实现

稻米供应链信息监管系统采用 Hyperledger Fabric 开源区块链平台实现供应链区块链网络构建,并利用云数据库对象存储模式进行相关数据存储,系统以 Golang、Jave、JavaScript 作为主要编程语言,并使用 Gin、Vue 作为前、后端框架进行全平台开发。系统本质即为供应链节点用户通过客户端界面

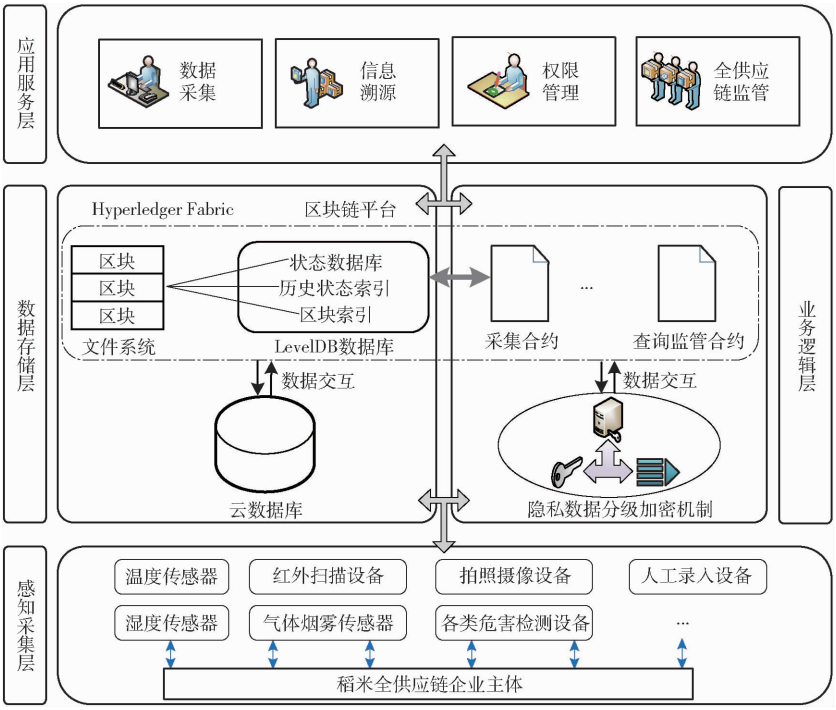


图 5　系统架构

Fig. 5　System architecture

对区块链账本和云数据库的上传和查询(监管)操作,信息监管流程逻辑如图 6 所示。

系统用户通过 Web 界面填写和传感器采集相关数据信息,然后向服务器发送数据上传请求,服务器根据用户提供的数据信息和用户账户信息查询用户的权限,若满足权限,则调用对应的功能模块以根据请求判断需要使用的智能合约,以向区块链网络发起一个交易提案。Hyperledger Fabric 智能合约又被称为链码(Chaincode),交易提案可将本次数据上传所需的链码标识、链码方法、相关的参数和节点用户签名等信息发送给背书节点,背书节点为交易作担保,与交易进行签名背书,并与链码相绑定,在背书节点收到交易提案后,验证数字签名并检测用户的操作权限,若拥有权限,则响应请求,继而模拟执行链码并返回链码执行结果及各背书节点的证书认证机构签名。

当系统客户端收到背书节点返回信息之后,将会判断提案结果的一致性,并确认是否按指定背书策略执行。系统若有足够的节点背书,应用程序客户端将会把数据打包到一起组成一个交易并签名,发送给排序节点,否则将会中止操作。区块链网络中的排序节点负责从全网的客户端接受交易,然后将交易按一定规则排序。在本系统中,排序节点将 Kafka 分布式系统对交易进行共识排序,然后按照区块生成策略生成新的区块,并发送给记账节点;记账节点验证交易有效性后记录交易,其在收到区块后,会对区块中的每笔交易信息进行校验,检查交易的输入输出是否符合当前区块链网络的状态,当校验完成后将区块追加到本地的区块链,并修改当前世界状态,之后其它用户节点会同步更新系统本地

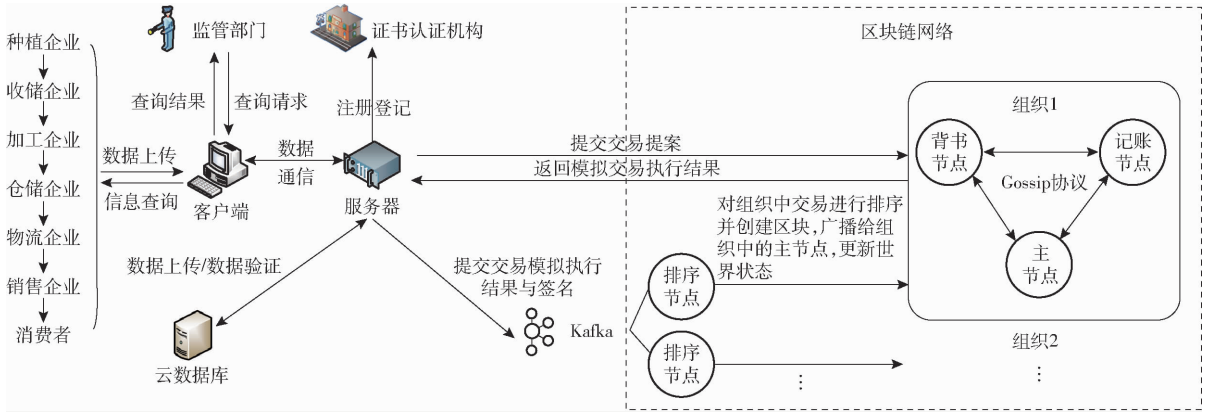


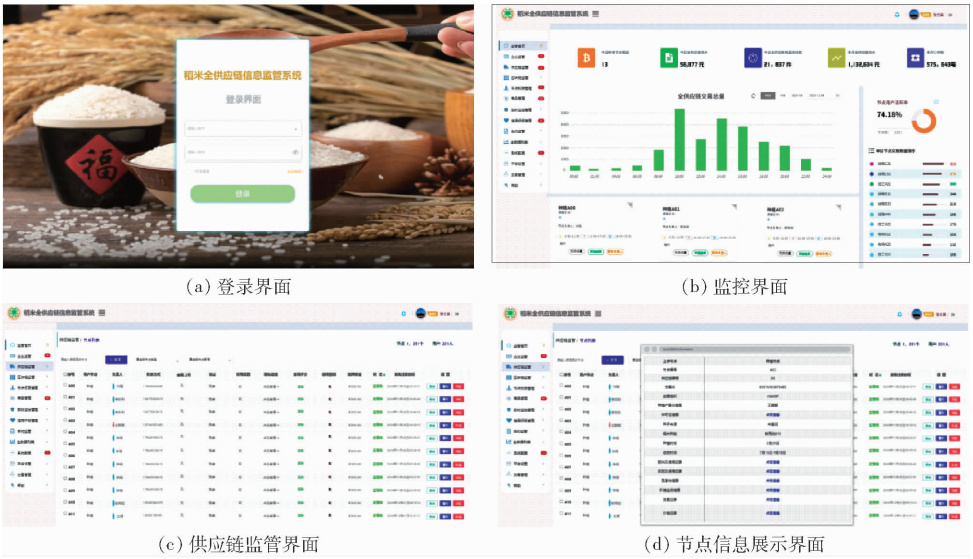
图 6　稻米供应链信息监管流程逻辑图

Fig. 6　Information supervision processes logic of rice supply chain

区块链网络信息,以完成数据上链。与此同时,数据加密传入云数据库,完成数据上云。

4.3 案例分析

通过对湖南省常德市某粮油企业下的稻米供应链进行调研,该企业旗下产业涉及稻米供应链所有环节,并且各环节监测与检验设备齐全,数据记录详细且留存完整。但由于各环节分属不同子企业,信息传输存在壁垒,并且之间业务交流繁多,导致监管难度进一步增大,因此选择采用本文所研发稻米供应链监管系统优化该企业对其稻米供应链的监督与管理。系统 Web 端界面如图 7 所示,图 7a 为监管系统登录界面,拥有管理员权限的监管者用户登录系统后能够对稻米供应链信息流动进行监督与管理。系统监控主界面如图 7b 所示,系统将供应链信息进行可视化处理,包括供应链节点交易总量、活跃节点用户及新增节点数目等,监管者用户可以查看当前稻米供应链运行状况,并且实时监控各企业主体节点上链信息。供应链监管包含稻米供应链所有用户节点详细信息列表,便于监管者检索各用户信息,如图 7c 所示。由于监管节点在系统链码中被写入最高权限,因此监管用户可以在系统中查询某一用户节点全部信息,包括其主体信息、基本信息、危害物信息、环境监测信息、交易记录和价格信息等,如图 7d 所示。所有查询信息皆为供应链企业主体数据经系统加密上传至区块链网络与云数据库后,系统再次进行解密后的数据明文,以保证数据存储传输过程中安全与隐私。而企业用户登录后除去增加数据上传功能外,在信息查询方面,仅可以在发送查询请求被同意的条件下对所在供应链上其他企业的公共数据与一级隐私数据进行查询,这样有效划分了监管者与企业用户的系统功能界限,便于权限管理,进一步保证了系统中数据流通安全。



(a) 登录界面 (b) 监控界面

(c) 供应链监管界面 (d) 节点信息展示界面

图 7 系统 Web 端界面

Fig. 7 Web interface of system

系统移动端为供应链中消费者所设计,其界面如图 8 所示。图 8a 为用户登录界面,登录后对稻米产品标注二维码进行扫描,以获取稻米供应链除交易记录和价格信息外全部溯源信息;如图 8b 所示,所有信息都是系统解密后明文数据。移动端功能设计简洁、针对性强,其溯源内容与企业查询产品内容相同,消费者可以准确快速了解到所购商品信息。

(a) 登录界面 (b) 信息溯源界面

图 8 系统移动端界面

Fig. 8 Mobile interface of system

5 结论

(1)通过对稻米供应链业务流程及流转特性进行全方位分析,进而抽象出稻米供应链的典型环节,并在此基础上构建了全链条各环节关键信息分类表。

(2)应用对称加密算法与散列加密算法提出隐私数据分级加密模式,设计了基于智能合约的监管业务逻辑方案,并以二者为基础结合云数据库构建

基于区块链技术的稻米供应链信息监管模型，设计并实现了稻米供应链信息监管原型系统，并结合实际案例对系统进行了分析。

(3)构建的稻米供应链信息监管模型及原型系统能够解决稻米供应链数据隐私加密、安全存储及权限管理等问题，实现了供应链信息互联互通和有效监管。本文研究可为粮油质量安全监管提供一种可行务实的应用方法。

参 考 文 献

[1] 袁隆平. 请别再向超级稻泼脏水[J]. 新湘评论，2016(2)：1.

[2] LI H, LUO N, LI Y W, et al. Cadmium in rice: transport mechanisms, influencing factors, and minimizing measures[J]. Environmental Pollution, 2017, 224: 622 - 630.

[3] 石少龙. 中国大米安全风险分析[J]. 中国稻米，2020，26(1)：6 - 10.

[4] MUTHAYYA S, SUGIMOTO J D, MONTGOMERY S, et al. An overview of global rice production, supply, trade, and consumption[J]. Annals of the New York Academy of Sciences, 2014, 1324(1): 7 - 14.

[5] JIFROUDI S, TEIMOURY E, BARZINPOUR F. Designing and planning a rice-supply-chain: a case study for Iran farmlands [J]. Decision Science Letters, 2020, 9(2): 163 - 180.

[6] ZHANG X, SUN P, XU J, et al. Blockchain-based safety management system for the grain supply chain[J]. IEEE Access, 2020, 8: 36398 - 36410.

[7] LAWSON B, POTTER A, PIL F K, et al. Supply chain disruptions: the influence of industry and geography on firm reaction speed[J]. International Journal of Operations & Production Management, 2019, 39(9/10): 1076 - 1098.

[8] KITTIPANYA-NGAM P, TAN K H. A framework for food supply chain digitalization: lessons from Thailand[J]. Production Planning & Control, 2020, 31(2 - 3): 158 - 172.

[9] 杨信廷，王明亭，徐大明，等. 基于区块链的农产品追溯系统信息存储模型与查询方法[J]. 农业工程学报，2019，35(22)：323 - 330.
YANG Xinting, WANG Mingting, XU Daming, et al. Data storage and query method of agricultural products traceability information based on blockchain[J]. Transactions of the CSAE, 2019, 35(22): 323 - 330. (in Chinese)

[10] 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. Modern 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? file_no = 2017s059&flag = 1. DOI: 10.6041/j.issn.1000-1298.2017.S0.059. (in Chinese)

[11] 孙传恒，于华竞，徐大明，等. 农产品供应链区块链追溯技术研究进展与展望[J/OL]. 农业机械学报，2021，52(1)：1 - 13.
SUN Chuanheng, YU Huajing, XU Daming, et al. Review and prospect of agri-products supply chain traceability based on blockchain technology[J/OL]. Transactions of the Chinese Society for Agricultural Machinery, 2021, 52(1): 1 - 13. http://www.j-csam.org/jcsam/ch/reader/view_abstract.aspx? file_no = 20210101&flag = 1. DOI: 10.6041/j.issn.1000-1298.2021.01.001. (in Chinese)

[12] GRECUCCIO J, GIUSTO E, FIORI F, et al. Combining blockchain and IoT: food-chain traceability and beyond[J]. Energies, 2020, 13(15): 3820 - 3838.

[13] 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)

[14] 郑雪静，熊航. 区块链如何促进数据要素的价值实现：以食品供应链为例[J]. 农业大数据学报，2020，2(3)：13 - 20.
ZHENG Xuejing, XIONG Hang. How the blockchain technology facilitate data to realize value: the case of food supply chain [J]. Journal of Agricultural Big Data, 2020, 2(3): 13 - 20. (in Chinese)

[15] 许继平，孙鹏程，张新，等. 基于区块链的粮油食品供应链信息安全管理原型系统[J/OL]. 农业机械学报，2020，51(2)：341 - 349.
XU Jiping, SUN Pengcheng, ZHANG Xin, et al. Prototype system of information security management of cereal and oil food whole supply chain based on blockchain[J/OL]. Transactions of the Chinese Society for Agricultural Machinery, 2020, 51(2): 341 - 349. http://www.j-csam.org/jcsam/ch/reader/view_abstract.aspx? file_no = 2002037&flag = 1. DOI: 10.6041/j.issn.1000-1298.2020.02.037. (in Chinese)

[16] 董云峰，张新，许继平，等. 基于区块链的粮油食品供应链可信追溯模型[J]. 食品科学，2020，41(9)：30 - 36.
DONG Yunfeng, ZHANG Xin, XU Jiping, et al. Blockchain-based traceability model for grains and oils whole supply chain[J]. Food Science, 2020, 41(9): 30 - 36. (in Chinese)

[17] ANTONUCCI F, FIGORILLI S, COSTA C, et al. A review on blockchain applications in the agri-food sector[J]. Journal of the Science of Food and Agriculture, 2019, 99(14): 6129 - 6138.

[18] 于合龙，陈邦越，徐大明，等. 基于区块链的水稻供应链溯源信息保护模型研究[J/OL]. 农业机械学报，2020，51(8)：328 - 335.
YU Helong, CHEN Bangyue, XU Daming, et al. Modeling of rice supply chain traceability information protection based on block chain[J/OL]. Transactions of the Chinese Society for Agricultural Machinery, 2020, 51(8): 328 - 335. http://www.j-csam.org/jcsam/ch/reader/view_abstract.aspx? file_no = 20200836&flag = 1. DOI: 10.6041/j.issn.1000-1298.2020.08.036. (in Chinese)

[19] CREYDT M, FISCHER M. Blockchain and more-algorithm driven food traceability[J]. Food Control, 2019, 105(1): 45 - 51.

(下转第 101 页)

//www.j-csam.org/jcsam/ch/reader/view_abstract.aspx? file_no=20160719&flag=1. DOI:10.6041/j.issn.1000-1298.2016.07.019. (in Chinese)
[15] 李骅. 风筛式清选装置设计理论与方法研究[D]. 南京:南京农业大学,2012.
LI Hua. Research on design theory and method of air and screen cleaning device [D]. Nanjing: Nanjing Agricultural University, 2012. (in Chinese)
[16] 李德建. 大喂入量谷物收获机清选过程仿真研究[D]. 济南:济南大学,2020.
LI Dejian. Simulation research on cleaning process of large feed grain harvester [D]. Ji'nan: Jinan University, 2020. (in Chinese)
[17] 李洪昌,李耀明,唐忠,等. 风筛式清选装置振动筛上物料运动 CFD-DEM 数值模拟[J/OL]. 农业机械学报,2012,43(2):79-84.
LI Hongchang, LI Yaoming, TANG Zhong, et al. CFD-DEM numerical simulation of material movement on vibrating screen of air and screen cleaning device [J/OL]. Transactions of the Chinese Society for Agricultural Machinery, 2012,43(2): 79-84. http://www.j-csam.org/jcsam/ch/reader/view_abstract.aspx? file_no=20120217&flag=1. DOI:10.6041/j.issn.1000-1298.2012.02.017. (in Chinese)
[18] 张春艳. 基于支持向量数据描述的累积和控制图[D]. 天津:天津大学,2012.
ZHANG Chunyan. Cumulative sum control chart based on support vector data description [D]. Tianjin: Tianjin University, 2012. (in Chinese)
[19] 方瑞明. 支持向量机理论及其应用分析[M]. 北京:中国电力出版社,2007.
[20] 熊伟丽,徐保国. 基于 PSO 的 SVR 参数优化选择方法研究[J]. 系统仿真学报,2006,18(9):2442-2445.
XIONG Weili, XU Baoguo. Study on SVR parameter optimization method based on PSO [J]. Journal of System Simulation, 2006,18(9): 2442-2445. (in Chinese)
[21] 舒宗玉. 基于多目标混合粒子群算法的无人船全局路径规划[D]. 武汉:武汉理工大学,2017.
SHU Zongyu. Global path planning for unmanned ship based on multi-objective hybrid particle swarm optimization [D]. Wuhan: Wuhan University of Technology, 2017. (in Chinese)
[22] 郑金华,邹娟. 多目标进化优化[M]. 北京:科学出版社, 2007.
[23] ZITZLER E, LAUMANNNS M, THIELE L. SPEA2: improving the strength Pareto evolutionary algorithm[R]. Lausanne, Switzerland: Swiss Federal Institute of Technology, 2001.
[24] DAS I, DENNIS J E. A closer look at drawbacks of minimizing weighted sums of objectives for Pareto set generation in multicriteria optimization problems[J]. Structural Optimization, 1997, 14(1): 63-69.
[25] 吴崇友,丁为民,张敏,等. 油菜分段收获脱粒清选试验[J]. 农业机械学报,2010,41(8):72-76.
WU Chongyou, DING Weimin, ZHANG Min, et al. Experiment on threshing and cleaning of rape by stage harvest [J]. Transactions of the Chinese Society for Agricultural Machinery, 2010,41(8): 72-76. (in Chinese)

(上接第 211 页)

[20] YU B, ZHAN P, LEI M, et al. Food quality monitoring system based on smart contracts and evaluation models[J]. IEEE Access, 2020, 8: 12479-12490.
[21] 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)
[22] POURNADER M, SHI Y, SEURING S, et al. Blockchain applications in supply chains, transport and logistics: a systematic review of the literature[J]. International Journal of Production Research, 2020, 58(7): 2063-2081.
[23] FOSSO W S, KALA K J R, EPIE B R, et al. Bitcoin, blockchain and fintech: a systematic review and case studies in the supply chain[J]. Production Planning & Control, 2020, 31(2-3): 115-142.
[24] 王小云,于红波. SM3 密码杂凑算法[J]. 信息安全研究,2016,2(11):983-994.
WANG Xiaoyun, YU Hongbo. SM3 cryptographic hash algorithm[J]. Journal of Information Security Research,2016,2(11): 983-994. (in Chinese)
[25] 卜晓燕,张根耀,郭协潮. 基于 AES 算法实现对数据的加密[J]. 电子设计工程,2009,17(3):86-90.
BU Xiaoyan, ZHANG Genyao, GUO Xiechao. Encryption system about data based on AES algorithm[J]. Electronic Design Engineering,2009,17(3):86-90. (in Chinese)
[26] SZABO N. Formalizing and securing relationships on public networks[J]. First Monday, 1997, 2(9):1-21.
[27] 蔡晓晴,邓尧,张亮,等. 区块链原理及其核心技术[J]. 计算机学报,2021,44(1):84-131.
CAI Xiaoqing, DENG Yao, ZHANG Liang, et al. The principle and core technology of blockchain[J]. Chinese Journal of Computers,2021,44(1):84-131. (in Chinese)
[28] 高一琛,赵斌,张召. 面向以太坊的智能合约自动生成方法研究与实现[J]. 华东师范大学学报(自然科学版),2020,2020(5): 21-32.
GAO Yichen, ZHAO Bin, ZHANG Zhao. Research and implementation of a smart automatic contract generation method for Ethereum[J]. Journal of East China Normal University(Natural Science), 2020, 2020(5): 21-32. (in Chinese)