基于区块链技术的大米质量安全管理与溯源

张太阳[1]， 王震宇[2]， 崔晓晖[1]， 盛 铭[2]， 曾文彬[2]

[1](武汉大学 国家网络安全学院，湖北 武汉 430079)

[2](武汉珞樱联创信息科技有限公司，湖北 武汉 430079)

通讯作者: 崔晓辉, E-mail: xcui@whu.edu.cn

摘 要: 大米是中国最主要的粮食之一,大米的质量安全紧密关系着人民的生命健康.现在大米产业存在优质原始数据少、数据可靠性差、信息不对称等问题,产业链上各生产环节的数据不通,行业缺乏统一、权威的监管平台和可靠的溯源系统.本文提出通过建立大米全产业链联盟,结合传统数据库存储技术和区块链技术,打通大米全产业链,构建大米质量安全大数据库和大米食品质量安全管理与溯源系统;并设计了多角色协同、多链互联、非完全去中心化的大米质量安全区块链协同网络(blockchain collaborative network,简称BCN),以云数据库存储原始生产数据,用区块链存储原始数据的哈希值和第三方质检报告等信息,以适应大米实际生产的应用场景,满足高效监管和快速溯源的需求.利用区块链的公开性和不可篡改等特性解决行业数据可靠性差、信息不对称等问题,实现对大米全产业链的高效监管和大米质量安全的快速溯源,为大米质量安全保驾护航.

关键词: 食品安全;产业联盟;区块链;快速溯源

The Quality Safety Management and Traceability of Rice Based on Blockchain Technology

ZHANG tai-yang[1], WANG zhen-yu[2], CUI xiao-hui[1], SHENG ming[2], ZENG wen-bin[2],

[1](School of Cyber Science and Engineering, Wuhan University, Wuhan 430079, Chain)

[2](Wuhan Luoying Lianchuang Information Technology Limited Company, Wuhan 430079, Chain)

Abstract: Rice is one of the most important grains in China,The quality and safety of rice is closely related to people's life and health.Currently, there are a series of problems in the rice industry, such as the lack of high-quality data, poor data reliability and information asymmetry,data on the rice industry chain is not shared.The rice industry does not have an authoritative unified regulatory platform and traceability system.This paper proposes to build the rice whole industrial chain alliance, integrate the traditional database storage technology and blockchain technology, link the rice whole industrial chain, build the big database for rice quality and safety, and develop the rice quality and safety management and traceability system.In addition,build a multi-role collaboration, multi-chain interconnection and non-complete decentralization of rice quality security blockchain collaborative network.The original data is stored in the cloud database, and the hash code of the original data and third-party quality inspection report of product are stored in the blockchain to adapt to the application scenario of rice production and meet the demand of efficient supervision and rapid traceability. The openness and tamperability of blockchain technology are utilized to solve the problems of poor data reliability and information asymmetry in the rice industry, to realize efficient supervision of the whole rice industrial chain and fast tracing of rice quality and safety, and to protect rice quality and safety.

Key words: food safety;industry alliance;blockchain;rapid traceability

食品安全与人们的健康生活和社会安定密切相关,食品安全问题由来已久,近几年尤为突出,也更为人们所关注.地沟油事件、毒胶囊事件、致癌金针菇事件、大米重金属超标等一系列食品安全事件不断冲击着人们对食品安全的信心,不断挑战国家的法律底线,使得质量安全有保障的诚信企业也面临着消费者的信任危机[1,2].食品溯源系统是保障食品质量安全的一种有效手段[3],食品安全追踪溯源体系的建立为问题食品的快速召回、保障食品安全和规范市场秩序方面起到非常重要的作用[4].大米作为最主要的粮食之一,其质量安全紧密关系着人民的生命健康.大米全产业链包括种植、收获、干燥、仓储、加工、物流、经销等关键环节,涉及到的生产单位有种植者、物流公司、加工企业、经销商等.然而由于各生产单位数据不不共享共通,消费者缺乏获取食品信息的有效途径[5].现有针对大米质量安全的溯源体系存在原始数据少、信息不对称、数据可信度差、溯源平台的标准和技术不完善等问题[6],没有统一的权威认证机构和溯源体系[7].

区块链技术兴起于 2008 年本聪在密码学邮件组发表的论文《比特币: 一种点对点电子现金系统》[8],2015 美国学者梅兰妮.斯万在其著作《区块链:新经济蓝图及导读》[9]对区块链技术作了定义,指出区块链技术是密码学、分布式存储等技术相结合的技术,具有公开透明、去中心化、分布式存储等特点.区块链技术最早运用于电子货币,经过多年的发展,区块链技术在众多领域都有所应用[10].由于区块链具有隐私性、公开性和不可篡改等特点,区块链技术可以很好地应用于食品溯源[11].

针对大米产业存在的问题和区块链技术的特点,我们提出通过建立大米全产业链区块联盟,打通大米生产全产业链,实现大米全产业链数据的共通共享,建立统一、权威可靠的大米质量安全管理和溯源系统(rice quality safety management and traceability system,简称RQSS).将区块链技术与传统的关系型数据库存储相结合,用关系数据存储原始生产数据,用区块链存储带有生产者节点数字签名[16,17]

* 基金项目：中央高校基本科研业务费专项资金，武汉大学自主科研项目（2042017gf0035），武汉大学科技横向项目（食品安全区块链系统研发）

的原始生产数据的哈希值等数据校验信息.利用 hash 函数的单向性和抗碰撞性[18,19],将巨大的原始生产数据映射为几百比特的哈希值,这样不仅减轻了区块节点的存储压力,节约了大量的存储资源,也保护了生产者的数据隐私.本文采用多角色协同、多链互联、非完全去中心化的区块链协同网络(blockchain collaborative network,简称 BCN),与节点角色单一、单链且完全去中心化的区块链结构相比,BCN 有管理者节点、生产者节点、存储节点三种角色节点,三种角色的节点有不同的功能.管理者节点是 BCN 的"中央处理器",负责联盟成员管理、数据加密和数据打包等任务;生产者节点负责数据的采集、打包、上传;存储节点用于验证和存储区块.三种角色的节点相互协同维护区块链网络运行.

RQSS 实现了对大米种植、生产、仓库、销售、物流、防伪、防窜、消费者等环节的信息化管理.政府监管部门利用本系统可以对大米全产业链的每一个环节进行监管,既能提高管理效率,也能是使监管更细化、更准确.本系统为企业的生产管理和市场开拓提供了可靠的数据支撑,提高企业生产管理效率,提升企业的竞争优势.同时,系统为消费者提供了方便可靠的溯源通道,消费者只需要手机扫描产品包装上的二维码,即可以获取该产品的详细产品信息.RQSS 的运用具有较好的社会效益和经济效益,实现对大米的安全追溯,对大米质量安全进行有效管理, 恢复人民对食品安全的信心,维护食品的市场秩序,

1 方法

1.1 业务架构

大米质量安全管理和溯源系统的业务架构如图 1 所示.RQSS 采集大米从种植到消费全产业链各环节的生产数据,结合大米全产业链的结构特点,建立针对种植、仓储、加工、物流、经销等不同生产环节的数据采集系统.数据采集系统采集大米从"农田"到"餐桌"的全息生产数据,并将数据存储在云数据库,形成大米质量安全大数据库.同时,生产者节点对数据做哈希运算得到数据的哈希值和 Merkle 树[20],将数据的哈希值和 Merkle 数加上生产者节点的数字签名形成该批数据的数据校验包.管理者节点将数据校验包、生产者节点信息和数据库关联信息等打包成区块在保存对应区块链上,以保证数据的不可篡改性和不可抵赖性.

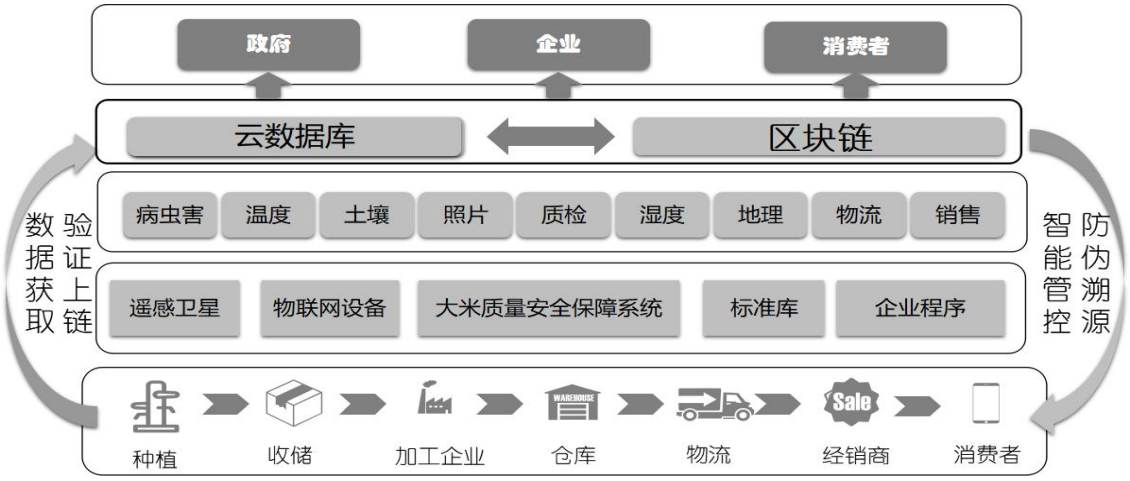

Fig.1 Business architecture diagram

图 1 业务架构图

基于大米质量安全大数据库和 BCN,政府可以对大米生产的每一个生产环节、每一个企业进行监管;企业通过全产业链的共享数据,可以调整和优化产能结构,提高生产和管理的效率;消费者通过 RQSS 查询产品从种植到消费所有的溯源信息.通过深度学习、数据挖掘等技术手段对数据进行分析,结合系统的标准库,RQSS 可以提供一系列的智能服务,如仓储智能监控、物流智能监控、加工智能监控等服务.

1.2 技术架构

为了契合大米全产业链生产应用场景、满足智能高效管理和快速溯源的需求,本区块链系统被设计为多角色协同、多链互联的非完全去中心化区块协同网络.如图 2 所示,系统的存储层是由云数据库和区块链组成,原始数据存储在数据库中,原始数据的哈希值和与数据库的关联信息等加密后存储在区块链上.在服务层,区块链节点根据功能不同分为管理者节点、生产者节点和存储节点三大类,管理者节点、生产者节点和存储节点共同协作维护区块链系统的运行.接口层连接服务层和功能层,功能层通过接口可以调用服务层的应用.在功能层有成员管理、数据采集、信用体系、追踪溯源等模块.用户层有企业、政府监管部门、消费者,不通用户可以根据自身的权限使用相应的功能和服务.

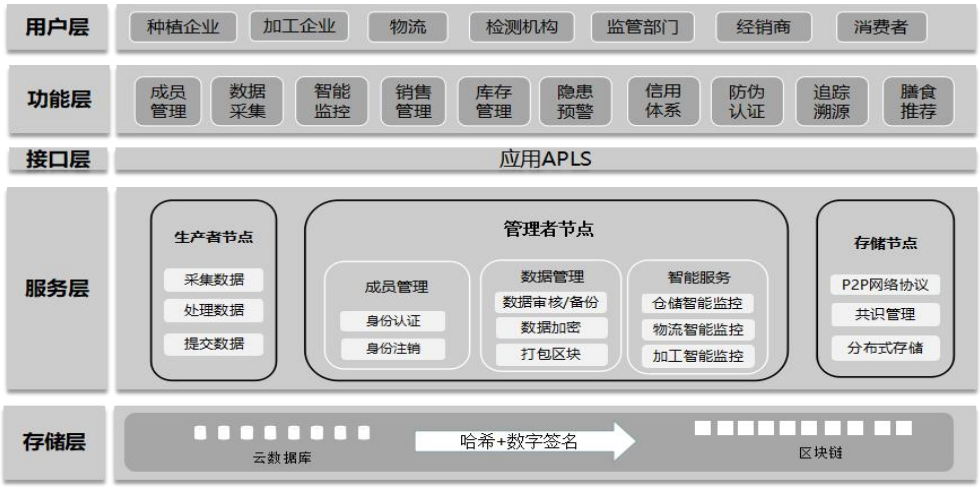

Fig.2　Technical framework

图 2　技术架构图

1.2.1 生产者节点

生产者节点对应于大米产业链上位于各生产环节的企业(即,联盟成员),负责数据的采集、处理和上传.根据所处大米产业链不同的生产环节,生产者节点可以分为种植节点、仓储节点、物流节点、加工节点、经销节点等.

为了保证大米全产业链数据的完整性和可靠性,建立一个高效、可信的大米质量安全保障系统,需要建立数据模型以采集大米全产业链全息生产数据.为保证数据的客观性和可靠性,模型中大部分数据是通过物联网感应设备采集,一小部分有人工录入.全息生产数据主要包括环境信息(地理、气候等),投入物信息(名称、成分、投入量等),物料属性信息(主要组成成分、关键危害因子等),控制信息(温度、浓度等技术参数),管理信息(责任人、管理制度、执行标准等)等.大米产业链关键数据见表 1.

Table 1　Rice whole industry chain key data acquisition model

表 1　大米全产业链关键数据采集模型

角色	生产节点	对象	主要数据
种植者	种植环境	产地	产权信息，经纬度
		气候	气候、空气、水质
		土壤	土壤环境、底肥
	栽培	种子	品种，厂家，采购日期，生产日期，保质期
			种子处理，环境条件
			发芽率,水分,净度,纯度
		水	水分，PH值，水温
		药品/肥料	品牌，厂家，采购日期，生产日期，保质期
			使用配方，使用剂量，使用时间
	收储	收割	收储企业，收割时间，收割天气
		干燥	干燥方式，干燥环境
		仓储	仓库信息，进仓品质，熏蒸条件，进出库水分，粮温
物流公司	稻谷出库	稻谷	车次编号，稻谷编号，运输条件，运输时间，出库记录等
加工企业	稻谷仓储	仓库	温度，湿度，卫生情况，仓管人员信息
		稻谷	稻谷编号，稻谷进出库质检报告，入出库数量，入出库日期
	加工	原料	投入品情况记录（水、食品级润滑油/脂、食品级包材）
		操作	生产/操作/包装车间人员健康证
	成品仓储	仓库	温度，湿度，卫生情况，仓管人员信息
		成品	成品编号，质检报告，入出库数量，入出库日期
物流公司	成品出库	成品	车次编号，成品编号，运输条件，运输时间，出库记录等
经销商	经销	经销商	经销企业信息、资质信息
		经销	成品信息，成品流通信息

采集到数据后,生产者节点按产品批次对数据做哈希运算,得到数据的哈希值和 Merkle 树,将数据的哈希值和 Merkle 树加上生产者节点的数字签名形成数据校验包,加上数字签名是为了保证数据的不可抵赖性.把原始生产数据用管理者节点的公钥加密,最后把数据校验包和加密后的原始生产数据发送给管理者节点.

生产者节点采集数据和对数据的处理流程具体如下:

1)生产者节点通过大米全产业链信息采集系统采集对应生产环节的生产数据;

2)按生产批次对采集到的生产数据做哈希运算,得到该批生产数据的哈希值;

3)按更细的生产维度对这批数据做哈希运算,生成 Merkle 树;

4)给生产数据的哈希值和 Merkle 树加上生产者节点的数字签名(用生产者节点的私钥加密)生成数据校验包;

5)用管理者节点的公钥对原始生产数据加密,最后把加密后的数据和数据校验包发送给管理者节点.

用管理者节点的公钥对原始生产数据加密是为了保障数据在传输过程中的安全性,只有管理者节点用其私钥解密后才能获取原始生产数据信息.

以加工节点为例,其从采集到提交数据的处理流程如图 3.

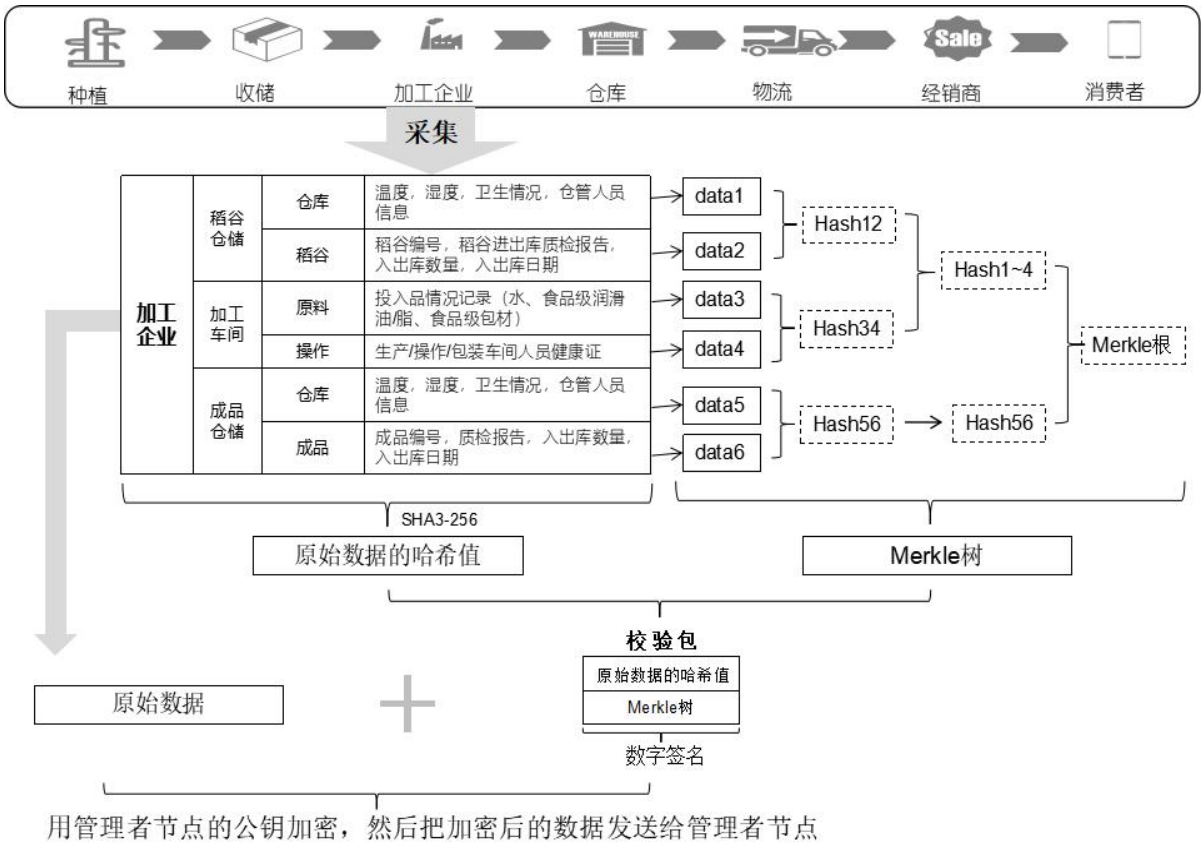

Fig.3 Process of processing data by processing nodes

图 3 加工节点对数据的处理流程

1.2.2 管理者节点

管理者节点由分布式服务器集群组成,是 BCN 的"中央处理器",管理者节点有成员管理、数据管理、智能服务三个功能模块.本文的区块链是联盟链,联盟成员即大米全产业链上的各个企业.成员管理模块负责联盟成员的身份认证和身份注销.新成员加入时,管理者节点对其身份进行审核、认证,联盟成员退出时,对其身份注销注销.

成员管理把公钥基础设施体系(public key infrastructure,简称 PKI)[21]和去中心化分布式存储的区块链网络组合在一起,将完全去中心化的非许可区块链转变成非完全去中心化的许可区块链.PKI 是一个基于公钥加密的框架体系,它不仅可以确保网络上的数据安全交换,还可以确认管理对方的身份.成员管理服务是成员身份认证中心,负责对成员进行身份审核、颁发身份认证证书及撤销认证.

当新成员要加入联盟时,先向管理者节点提出申请,审核通过后,成员管理服务中心会给新成员生成一个身份 ID 并且颁发一个身份认证证书.具体流程如下:

1)申请者(即生产者节点)生成属于自己的秘钥对,然后将申请者相关信息和申请者公钥加上申请者的私钥加密形成申请书;

2)申请者将申请书和申请者的公钥发送给管理者节点的成员管理服务中心;

3)审核人员对申请者的身份进行审核,如果审核通过,成员管理服务中心生成属于申请者的身份 ID 和身份认证证书;

4)成员管理服务中心将申请者的身份 ID 返回给申请者,同时将申请书和身份认证证书保存在数据仓库.

申请加入联盟和身份认证流程如图 4.

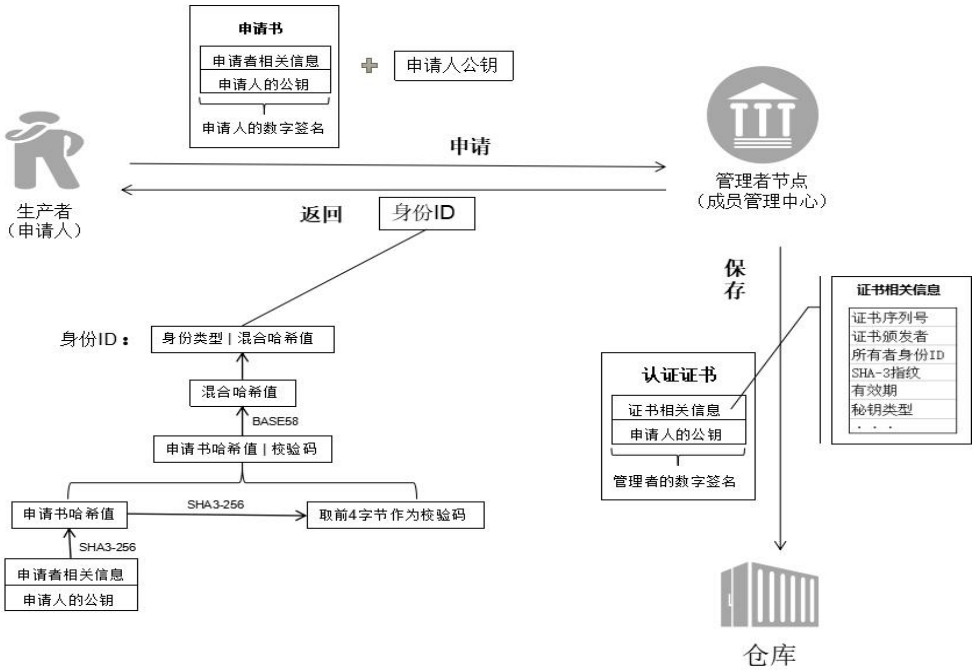

Fig.4　Identity authentication process

图 4　身份认证流程

身份 ID 是生产者节点(即,联盟成员)唯一的身份标识,由管理者节点生成.管理者节点对生产者的申请书做一系列的哈希运算的到混合哈希值,然后将身份类型号和混合哈希值组成生产者节点的身份 ID.

认证证书是联盟成员的有效身份凭证,证书包含申请者公钥、身份 ID、有效期等信息.证书由管理者节点颁发,并带有管理者节点的数字签名,身份认证证书将生产者节点的身份 ID 和公钥绑定在一起,在对生产者节点的身份认证的同时也对生产者节点的公钥进行了认证.身份认证证书有生产者节点的身份 ID 和被用管理者节点公钥加密后的申请书，不包含生产者节点的详细信息.管理者节点可以通过生产者节点的身份 ID 和申请书获取生产者节点的详细信息,其他用户因为没有管理者节点的私钥,所以无法获取生产者节点的详细信息,只能获取生产者节点的身份 ID,这样既保护了联盟成员信息,同时监管机构又能对企业进行监管.

当要对生产者节点身份的有效性进行验证时,需要从证书仓库下载生产者节点的认证证书,然后用管理者节点的公钥解密,结合证书作废清单(certificate revocation list,简称 CRL)才能对生产者节点身份的有效性进行验证.联盟成员要退出联盟时,成员管理服务中心需要在 CRL 上添加该成员的身份 ID 和证书序列号,完成对该成员的身份注销操作.

管理者节点对数据的管理操作包括接受对生产者节点发送过来的数据并进行校验审核,审核通过后,将原始生产数据保存在云数据库中,然后将生产者节点信息、数据校验包以及与数据库关联信息打包成区块发送到区块链网络.数据校验包是带有生产者节点数字签名的原始数据的哈希值和 Merkle 树,原始数据的哈希值被用于检验存储在云数据库的原始数据是否被篡改,Merkle 树用于判断数据的那个部分被篡改.将原始生产数据保存在云数据库中,只将原始数据的校验信息存储区块链上,这样做既是为了减轻区块存储节点的存储压力、较少空间浪费,也是为了提高系统的溯源速度,因为在传统数据库中数据查询的速度要比在区块链上的数据查询速度快很多.

管理者节点对生产者节点提交的数据具体处理流程如下:

1)用管理者节点的私钥和生产者节点的公钥对生产者节点发送过来的数据依次解密;

2)对解密后的数据进行审核校验，检查数据的完整性和一致性,对原始生产数据做哈希运算,将得到的哈希值与生产者节点发来的哈希值做对比,如果哈希值相等并且数据完整,则数据通过审核;

3)数据审核通过后，管理者节点对原始生产数据、生产者节点信息和时间戳做哈希运算得到哈希值,然后将区块的链号、区块号和该哈希值拼接组成这批数据的数据 ID;

4)将带有生产者节点数字签名的数据校验包、与云数据库的关联信息、质检报告等打包成区块,并将区块广播到区块链网络中,由区块链网络上的存储节点把区块加入到相应的区块链上.

管理者节点对数据校验包、生产者节点的身份 ID 以及盐一起做哈希运算得到哈希值,然后再把链号、区块号与得到的哈希值拼

接组成该批数据的数据 ID.数据 ID 是区块与云数据库关联的关键值,通过数据 ID 和保存在区块中与云数据库的关联信息可以查询到该数据 ID 对应的保存云数据库上的原始生产数据。

管理者节点生成的区块结构如图 5.

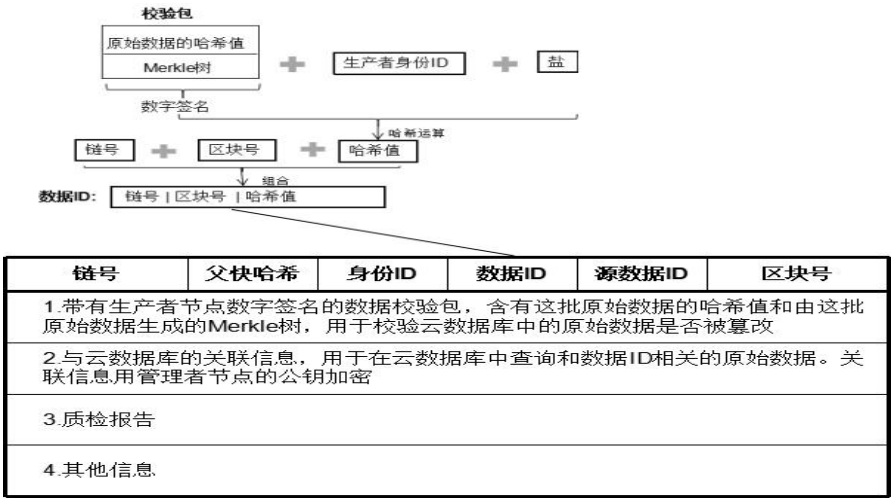

Fig.5 Block structure

图 5 区块结构

区块由区块头和区块体组成。区块头由链号、父块哈希、身份 ID、数据 ID、源数据 ID 和区块号组成.区块体包含带有生产者节点数字签名的数据校验包、区块与云数据库的关联信息、质检报告等信息.

1.2.3 存储节点

存储节点即存储区块的 peer 节点,由这些 peer 节点组成区块链 P2P 网络.P2P 网络中的 peer 节点,地位平等,无主从之分[22].区块链 P2P 网络提供共识管理、分布式账本、P2P 网络协议等服务.

存储节点负责对区块进行验证和存储.当 P2P 网络接收到管理者节点打包的区块,peer 节点会对该区块进行验证,验证通过后依据共识协议把区块加入对应的区块链上.共识协议保证了 P2P 网络上各节点存储的区块内容一致性.验证区块时,先用管理者节点的公钥解密校验包,然后用生产者节点的公钥解密数据校验包,验证通过则将区块加入到对应的区块链上.区块中的数据校验包带有管理者节点和生产者节点两方的数字签名,保障了区块的合法性和不可抵赖性.

根据存储数据来源不同,本文中的区块链系统有种植链、稻谷仓储链、稻谷运输链、稻谷经销链、加工链、成品仓储链、成品运输链、成品经销链 8 条链,这 8 条区块链通过数据 ID 和源数据 ID 相互关联.多链互联的区块架构不仅使得系统结构清晰,也能有效加快溯源速度.图 6 为不同区块链的互联关系示意图.

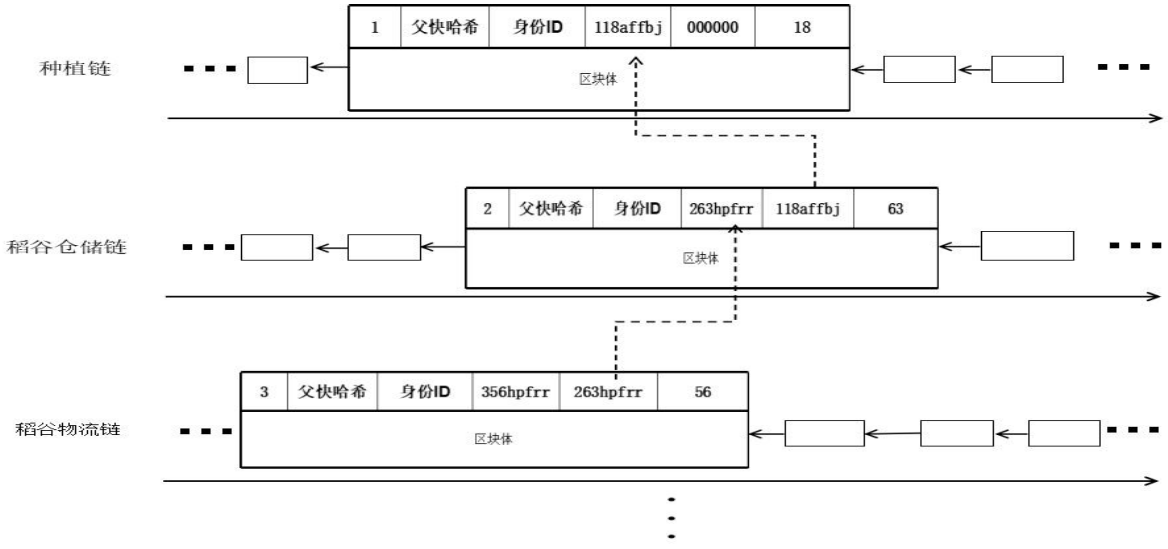

Fig.6 Correlation of different chains

图 6 多链互联

不同链上的区块通过数据 ID 和源数据 ID 进行关联.在溯源过程中,通过源数据 ID 号中的链号快速定位到母链(上一个生产环节所在的区块链),再按区块号用二分查找法在母链上快速找到母区块,通过母区块中的数据 ID 和云数据关联信息能在云数据库中查到与该数据 ID 对应的详细数据.依次往上溯源,直到源数据 ID 为 0 则代表已溯源到最原始位置,溯源结束.

因为区块链上的链号是从小到大依次增长的,所以可以用二分茶渣的方法快速定位到要查找的区块,查找到区块后,通过区块的数据 ID 和数据库关联信息可以快速定位要查找数据在云数据库的位置.定位区块时用的是二分查找法,所以可以快速找到需要查找的区块,在区块链上查找区块的时间复杂度为 log2(N),N 为区块链的长度.

2 结果与讨论

2.1 溯源方法和溯源要素

大米质量安全溯源方法按溯源方向可分为逆向溯源和顺向溯源.逆向溯源指沿产业链起点(种植)到产业链终点(消费)的方向进行的溯源,顺向溯源指沿产业链终点(消费)到产业链起点(种植)的方向进行的溯源.

溯源系统的性能评价有宽度、深度、密度 3 个维度.宽度是指信息量大,本溯源系统采集了大米产业链的全息生产数据,包括营养性、安全性、环境、工艺、管理等信息,达到 100 种以上.深度是指产业链涵盖生产节点范围,本系统涵盖大米全产业链从种植到消费所有关键节点,包括种植、收获、干燥、仓储、加工、物流、经销.密度是指生产环节距离和数据采用频率,距离短,频率大的密度就高.

溯源方法有四要素:产品标识,追溯工具,产品信息,路径信息.本溯源系统的溯源四要素具体如图 7.

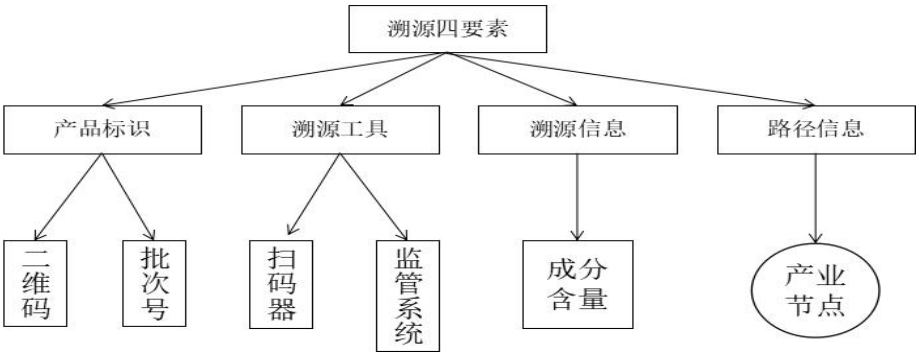

Fig.7 Four elements of traceability

图 7 溯源四要素

批次号(即产品的数据 ID),由区块链链号、区块号和生产数据的哈希值组成.二维码与产品批次号对应,通过二维码可以解析出产品批次号和溯源网页超链接,从而查到产品的详细溯源信息.二维码和溯源之间的关系如图 8.

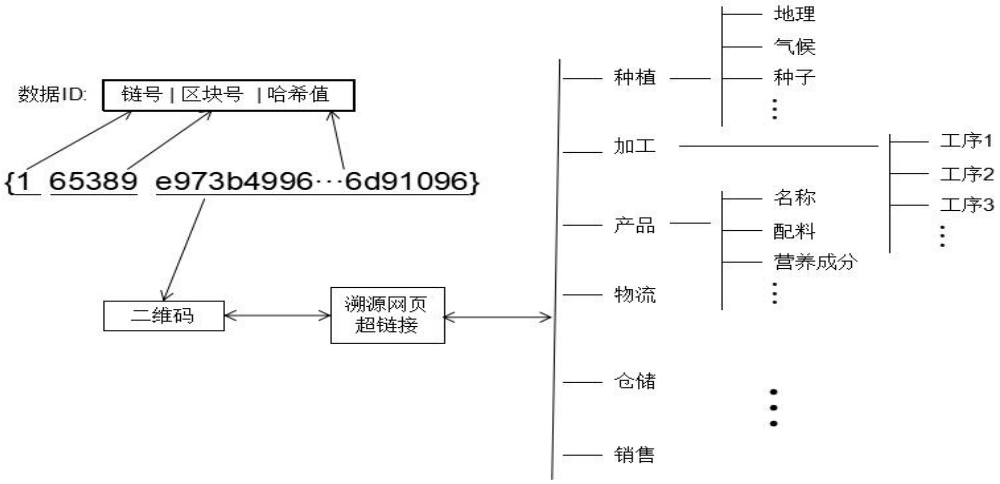

Fig.8 The relationship between qr code and traceability

图 8 二维码与溯源

2.2 溯源过程

政府监管部门通过溯源系统,在溯源界面用产品批次号进行溯源,沿产业链起点(种植)到产业链终点(消费)的方向溯源.为了保护企业的隐私和利益,只有政府监管部门有权限对大米全产业链进行逆向溯源.政府监管部门通过逆向溯源的方式监控大米全产业链的全过程,进而对大米质量安全事件及时做好应对措施,防止问题大米的扩散,对已经流通的问题大米也能及时召回.

逆向溯源时,溯源系统通过产品的数据 ID 在云数据库中查出数据 ID 对应的生产数据,对查到数据做哈希运算;然后在区块链中找到与该数据 ID 对应的区块,解密区块的校验内容,将云数据数据的哈希值和区块的校验哈希值做对比,如果两者的哈希值相等,则说明云数据库中的数据没有被篡改,为可信数据.沿着关联的数据 ID 依次向后溯源,直到产品最后的流通环节,完成溯源,最后将溯源信息返回给溯源信息展示界面.

消费者通过二维码阅读器扫描产品二维码进行溯源,沿产业链终点(消费)到产业链起点(种植)的方向溯源.扫码器解析二维码,得到溯源网页超级链接地址和产品的数据 ID,然后把数据 ID 按溯源地址发给溯源系统;溯源系统在云数据库中查出数据 ID 对应的生产数据;通过数据 ID 在区块链中找到对应的区块,解密区块信息;然后根据区块的校验包和数字签名验证云数据库的数据是否被篡改;依据区块中的源数据 ID 向前溯源，重复上面的数据查找、校验过程等操作,直到区块的源数据 ID 为 0 代表溯源结束,最后将溯源信息返回给扫码器.

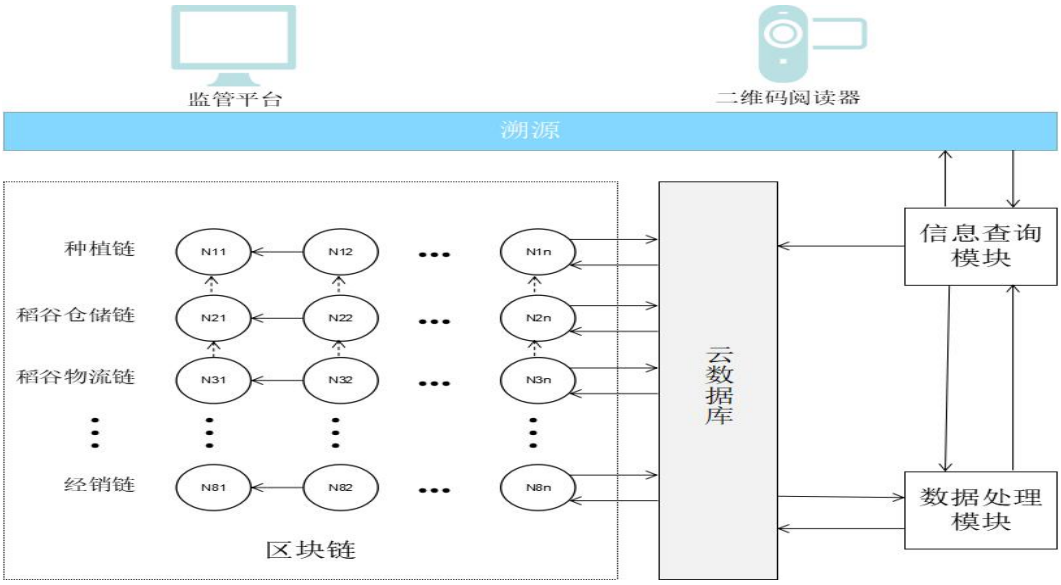

Fig.9 traceability system

图 9 溯源系统

3 结论和展望

通过产业联盟的方式打通大米全产业链,建立大米质量安全大数据库,将区块链技术运用在大米质量安全管理和溯源中,利用区块链的透明性和不可篡改性解决行业信息不对称、数据造假等问题.用云数据库存储大米的原始生产数据,区块链存储原始生产数据的哈希值等校验信息和生产者节点的相关信息.RQSS 综合了云数据库和区块链的优点,用传统的关系型数据库海量原始生产数据,仅将数据校验信息、生产者节点信息和质检报告等少量数据存储在区块链上,区块链的不可篡改和分布式存储等特性保证云数据库中数据的可信性,这样既减小了区块链的存储压力,也能保证数据的可靠性,实现快速溯源.

利用大米质量安全大数据库,政府可以有效的监管大米生产的每一个环节,对大米质量安全做到及时、准确地管控;企业可以根据联盟数据优化产业结构,提升企业竞争力,树立良好的品牌形象;消费者能够方便地获取可信、详细的溯源信息,建立消费者和食品企业的信任关系.利用机器学习、数据挖掘等手段还可以实现对产业链的智能管控,提供大米品质预测、安全隐患预警等服务.

References:

[8] Bitcoin:a peer-to-peer electronic cash system[Online]. Nakamoto S. https://bitcoin.org/bitcoin.pdf . 2009.

[9] Melanie Swan M.Blockchain:blueprint for a new economy[M].USA:O’Reilly,2015.

[12]Pilkington M.Blockchain technology:principles and applications[J].Research Handbook on Digital Transformations,edited by F.Xavier Olleros and Majlinda Zhegu.Edward,2016.

[13] Antonopoulos,Andreas M. Mastering Bitcoin.O'Reilly Media,Inc,2014.

[14] Buterin,Vitalik.Ethereum:A Next-Generation Smart Contract and Decentralized Application Platform[EB/OL].https://github.com/ethereum/wiki/White-Paper,2013.
[15] Buterin,Vitalik.Ethereum Yellow Paper[EB/OL].https://github.com/ethereum/yellowpaper,2014.
[16] Koblitz N.Elliptic curve cryptosystems[J].Mathematics of Computation,1987,48(177):203-209.
[17] Miller V S.Use of Elliptic Curves in Cryptography[C].International cryptology conference,1985:417-426.
[18]Andoni,Alexandr,Indyk,Piotr.Near-optimal hashing algorithms for approximate nearest neighbor in high dimensions[J].COMMUNICATIONS OF THE ACM,2008,51(1):117-122.
[19] SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf[EB/OL],2015.
[20] Coron JS,Dodis Y,Malinaud C.Merkle-damgard revisited: How to construct a hash function[J].Lecture Notes in computer Science,2005,(3621):430-448.
[21] Symantec Digital IDs for secure Email[EB/OL].http://ww.symantec.com/digital-id,2017
[22] Daniel L,Charles H,Stan L.Bitshare:A Peer-to-peer Polymorphic Digital Asset Exchange[J].Self-published paper,2013(9),11.

附中文参考文献:

[1] 孙兴权,姚佳,韩慧等.中国食品安全问题现状、成因及对策研究[J] .食品安全质量检测学报,2015(1).
[2] 孙宝国,王静,孙金沅.中国食品安全问题与思考[J].中国食品学报,2013,13(5):1-5
[3] 白红武, 孙传恒, 丁维荣, 等.农产品溯源系统研究进展[J].江苏农业科学, 2013 (04) :1-4.
[4] 钱丽丽,于果,迟晓星等.农产品产地溯源技术研究进展[J].食品工业,2018(1).
[5] 张晓玲,方逵等.大米追溯系统研究现状及发展趋势[J].农业网络信息,2013(6).
[6] 陈芳,姜启军.基于信息不对称的食品追溯体系的研究[J].黑龙江农业科学,2011,(9),112-115.
[7] 刘璐,窦晓涵,曹树贵.基于国内外农产品溯源发展现状推进我国农产品溯源的发展[j].河北企业,2017(07).
[10] 袁勇,王飞跃.区块链技术发展现状与展望[J].自动化学报,2016,(4):481-493.
[11]孙志国,李秀峰,王文生,冀智强.区块链技术在食品安全领域的应用展望[J].农业网络信息,2016,(12):30-31.