基于区块链的农资交易溯源系统的设计研究

黄系盟[1,2],赵应丁[1,2*],李求德[1,2]

(1.江西农业大学软件学院,江西南昌 330044;2.江西省高等学校农业信息技术重点实验室,江西南昌 330044)

摘要 农资作为农业生产中重要的补给品,其交易信任问题一直以来都受到社会的关注。为了确保农资质量合格,需要对农资供应链信息进行溯源管理。利用区块链技术,分析了农资供应链各环节需求,搭建了一套农资交易可信品控溯源系统。最后,通过试验表明单位上链时间并不随溯源数据规模变大而变大,说明区块链在溯源系统上的应用具有安全性和稳定性。

关键词 质量溯源;区块链;去中心化;分布式存储

中图分类号 TP 399 **文献标识码** A

文章编号 0517-6611(2022)08-0227-05

doi:10.3969/j.issn.0517-6611.2022.08.060

开放科学(资源服务)标识码(OSID):

Design and Research of Agricultural Materials Transaction Traceability System Based on Blockchain

HUANG Xi-meng[1,2],ZHAO Ying-ding[1,2],LI Qiu-de[1,2] (1.School of Software,Jiangxi Agricultural University,Nanchang,Jiangxi 330044;2.Key Laboratory of Agricultural Information Technology of Colleges and Universities in Jiangxi Province,Nanchang,Jiangxi 330044)

Abstract As an important supplement in agricultural production,the transaction trust of agricultural means has always been concerned by the society.In order to ensure the quality of agricultural means,it is necessary to carry out traceability management of agricultural means supply chain information.We used blockchain technology to analyze the demand of each link in the supply chain of agricultural means,and built a set of trusted quality control traceability system of agricultural means transaction.Finally,the experiment showed that the unit time on the chain did not increase with the size of traceability data,which showed that the blockchain had security and stability.

Key words Quality traceability;Blockchain;Decentralization;Distributed storage

农资是农业生产中重要的投入品和补给品,其质量是发展现代农业的基础和前提,是农业生产作业的重要组成部分,历来受到国家的高度重视。近年来,国内农资质量安全问题事件屡屡发生,这引起了社会和人民较大的关注[1]。农民从事生产作业时,无法保证自己购买的种子和农药等生产资料是否合格,因此解决农资交易信任问题是一项非常重要的任务。

一般来说,现在可以使用溯源系统平台将农资产品的数据上传至云端,通过给消费者提供溯源服务来查询产品来源,以此来解决交易信任危机[2]。区块链具有不可篡改、去中心化、公开透明等特性,是当前最适合存储这种数据的存储方法。最近几年,很多国内外的学者在信息技术、物联网、区块链等技术上对溯源系统进行相关研究并取得了一些成果。2013 年黄庆等[3]通过对物联网相关技术及网络体系架构的分析,展示了其在农资产品溯源服务系统上的应用可实现对农资产品的溯源防伪。2017 年郑开涛等[4]提出了基于时空追溯码的农产品质量安全溯源多边平台,并对该平台进行了总体设计以提高农产品追溯效率。2020 年吴晓彤[5]针对传统溯源系统一般是以中心数据库为基础的溯源模式出现的信任问题,提出基于区块链的农产品溯源系统。对于最近几年刚提出的比较多的基于区块链的农产品溯源系统,同样可适用于农资供应链上。鉴于此,笔者在分析传统农资溯源系统的基础上,针对农资溯源系统存在的问题,提出利用区块链的去中心化等特性,将农资溯源信息存储在各个节点上,来解决溯源信息安全性问题,使用 Fabric 框架实现了基于区块链农资交易溯源系统,该系统实现了农资溯源信息的安全性。

1 农资溯源研究分析

1.1 农资的概念 农资指的是农业生产过程中所用到的物质资料,比如农药、种子、农膜、农机等,它所覆盖的范围比较广泛[6]。

1.2 农资溯源的必要性 农资作为农业生产必不可少的生产资料,与“三农”服务也有千丝万缕的关系[7]。溯源往往是为了使得消费者农资溯源为产品质量进行可信背书,消除了消费者对产品安全的顾虑,对生产商建立足够的信任。最近国内农资产品假冒问题屡屡发生,使得农资产业链出现信任危机,如何解决消费者和生产商的信任问题、重新建立行业信任体系,是当前我们需要去解决的事情。

1.3 传统农资溯源现状及问题分析 纵观国内溯源平台,目前运行的农资溯源系统较多,以 2017 年上线的“中国农资质量追溯平台”为例,它结合物联网、标识技术,率先在我国农资行业中建立全国统一的农资质量追溯平台[8]。通过该平台,消费者可以删除查询农资信息;生产者可以对农资产品流通环节和出入库环节进行管理;农资流通企业可以获得产业环节的数据;监管部门可以通过该平台进行监督管理。其他的农资质量溯源系统都大同小异,使得我国农资质量安全追溯体系快速发展。但是这些农资溯源系统仍然有很多不足,比如数据安全问题、运营成本过大。

1.4 区块链技术在农资质量安全追溯体系的应用 由于区块链具有很多传统技术不具备的特征,比如不可篡改、去中心化等,考虑到传统农资质量追溯系统的一些不足,区块链可以给它带来一些针对性的解决方案。首先是去中心化,传

基金项目 国家重点研发计划课题(2020YFD1100605)。

作者简介 黄系盟(1996—),男,江西宜春人,硕士研究生,研究方向:区块链应用技术。*通信作者,教授,博士,硕士生导师,从事区块链应用技术、自然场景计算机可视化建模研究。

收稿日期 2021-07-23;**修回日期** 2021-08-25

统的农资溯源系统一般是接入云服务器,它具有强大的运行和存储能力,录入的数据量不是很巨大时,云服务器能够处理。但是当数据量越来越大时,中心服务器的处理能力有限,很有可能会死机或者崩溃,计算难以进行存储和运行。另外,中心化的服务器设备运营成本比较高[9]。

2 相关技术

2.1 区块链概述 区块链从狭义上来说是一种链式存储结构,由一个一个区块连接而成,区块结构如图 1 所示,区块分为区块头和区块体,区块头包含版本号、前一区块的哈希、时间戳、随机数、目标哈希、merkle 根,区块体保存了交易记录,是以 Merkle 树的方式存储,Merkle 根存储了所有交易记录的哈希值,它存在区块头上[10]。

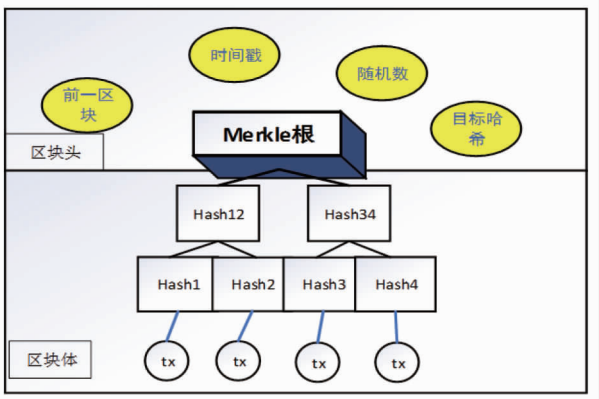

图 1 区块结构

Fig.1 Block structure

广义上区块链是一种分布式存储的方式,它具有去中心化、不可篡改、不可逆、匿名等特性,所以这种概念广泛应用于金融、计算机等行业,比如比特币、以太坊等电子货币、分布式节点储存。另外,区块链有私有链、联盟链和公有链 3 种,私有链相当于由一个公司组成,仍然不存在中心节点,该公司不同节点由会计核心控制。公有链向全网公开,节点数量不限,他们按照激励机制相互竞争,为的是获取记账权。联盟链就是几个公司组成一个联盟(通道),节点们通过共识算法来达成一致,并广播同步消息[11]。

2.2 区块链关键技术

2.2.1 智能合约。智能合约,顾名思义就是一种契约,它通过信息化的方式验证,执行计算机合同。当人们规定好了规则之后,机器就自动执行,这样就不容易出现异常或者作恶[12]。区块链中的公开透明性质是智能合约赋予的,不可篡改性质是共识算法赋予的[13]。

智能合约将区块链应用在项目中,从而将数据库和现实连接起来。智能合约运行在区块链上面,可以在满足条件的情况下被触发。智能合约解决了不同系统之间的标准不一致的问题[14]。智能合约在很多地方都在应用,比如电子商务、供应链优化等场景。在农资溯源系统里,智能合约充当了合同的作用,当触发合同条件时,它会自动执行程序代码。

2.2.2 分布式存储。分布式存储的定义是将数据分散的存储在网络上,各个节点通过网络相连,然后对这些节点资源进行统一的管理,对外作为一个整体提供存储服务[15]。区块链的分布式存储打破了传统溯源系统数据存储中心化的局面,使信息分布式存储在多节点上,节点上的信息保存都比较完整,既增强了产业链各环节的信息互通性,也使得其去中心化、透明性、可溯源性和防篡改性的特点与农资溯源领域极为契合[16]。

2.2.3 共识机制。区块链中共识机制主要有 4 种类型:①PoW 工作量证明。PoW 是第一个共识算法,是由中本聪首次提出来的,能解决“双花攻击”问题。它是通过计算获得随机数,之后就拥有账本的记账权,并向其他节点广播账本信息,验证后在将账本复制下来。账本有一个评价指标,每个账本加入一个随机元素使得难度变化,确保时间内只有一个节点有权利记账。比特币中,节点算力越大,获得记账权的可能性越大[17]。②POS 权益证明。主要是为了争夺记账权,确保节点账本一致。POS 有个比较明显的缺点,就是节点在拼算力的过程中十分消耗资源,导致大量的资源浪费。POS 就完美弥补了这样的问题,它是按照持币的数量来决定记账的权力[18]。③DPOS 委托权益证明。通过特殊加密算法使得节点之间记账,DPOS 算法被证明能符合区块链的性能要求。DPOS 机制将每个币视为一张选举票,币的拥有者根据其持有的数量,投票给自己信任的委托人[19]。系统根据得票多少选出受托人。受托人的工作就是签署区块,且在每个区块被签署前,检验前一个区块的真伪。币的持有者将权益交给受托人,受托人也可以专心从事记账工作。

2.3 农资溯源服务相关技术 农资产品溯源服务技术包含众多,最终的目的就是农资产品的溯源信息,比如源头、运输、销售、使用等进行查询,可以利用先进的技术,使用很多种方式,如二维码、RFID、激光码等对农资产品录入信息,对农资产品进行跟踪,实现产品全周期管理。农资供应链环节有生产、仓储、分销、运输、监督及消费[20]。

传统农资溯源使用了一些方法技术来确保信息的安全性:①防伪号码,产品的真伪可以使用涂层材料来追溯,不过这种方法的追溯能力不够强,无法查询产品的运输和更换信息。②条形码[21-24],这是一种比较常见的可追溯性服务技术。产品表面印有数字和条形码,形成生产时间、生产批号、生产许可证、国家药品许可证等,但仍存在易被仿制的缺陷。二维码,使用农产品,用户可以通过扫描产品外观上打印的二维码来获取信息。③射频识别技术,与跟踪器或记录仪类似,农资产品进出仓时能自动读取和采集信息[25-27]。

以上技术的优势是:①近距离非接触识读,范围为十几厘米到几十米。②可以对抗比较恶劣的环境。③安全性比较强。④可以识别高速运动的物体。但是,缺点是这样的溯源方法成本比较高。

3 系统设计方案

该系统的目的是解决农资供应链数据安全、信任的问题,该研究提出的框架和解决方案将专注于在联盟链平台上自动执行的智能合约。智能合约将由通道中的几个节点进行执行,并由所有节点商定执行结果。另外,节点是区块链

网络的组成部分,它可以是收集、验证和执行事件的计算机器。该框架由所有节点商定执行结果。值得注意的是,挖掘节点是区块链网络的组成部分。节点可以是任何收集、验证和执行事务的计算机器。节点还将这些事务的数据和结果存储在 1 个账本中,该账本由所有节点复制和同步。在某种程度上,节点具有与所有其他节点完全相同的副本。区块链中,智能合约通过函数调用来接收交易,还将触发事件,可以在违规发生时进行监控、跟踪并进行警报。在所示这种情况下,解决方案特别关注农资供应链。参与实体包括生产商、运输商、分销商、零售商和最终客户。

3.1　系统环节设计　由图 2 可知,农资溯源供应链与农产品相类似,分为生产、流通、销售等环节,各环节相互协作可以保证溯源高效完成。该研究针对农资溯源供应链的需求,对各环节的应用进行了设计。

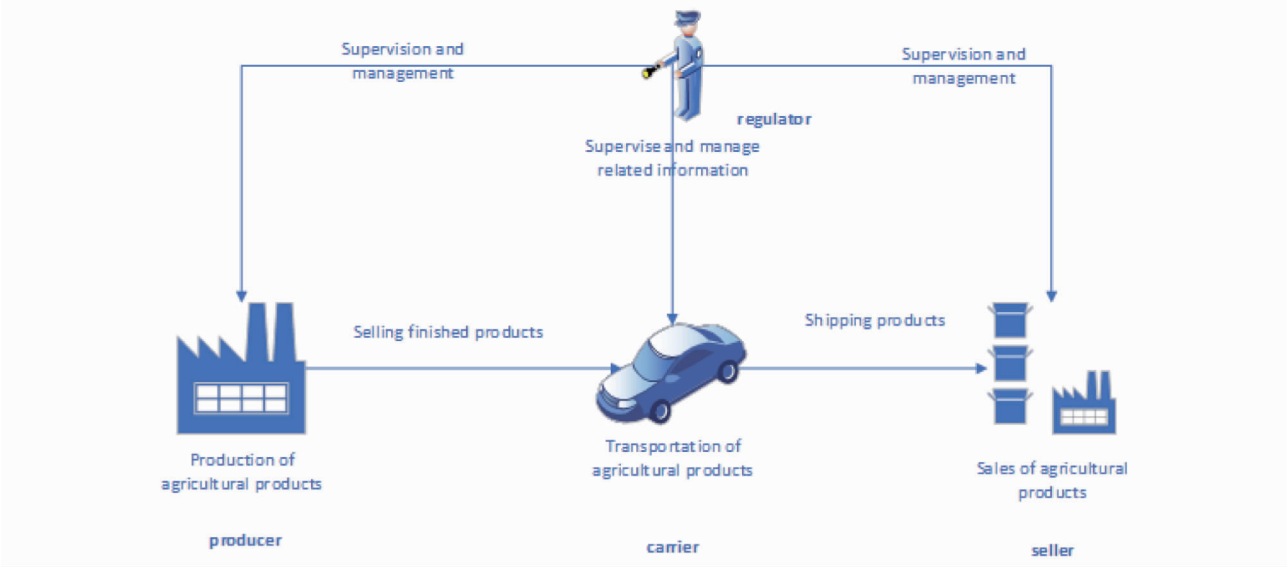

图 2　系统供应链流程示意图

Fig.2　System supply chain flow diagram

3.1.1　生产环节。主要节点是农资生产企业。节点输入产品信息并将信息上传到区块链上,由此构成创世区块。经过监管者审批之后在进行标记,生成独一无二的码。各节点通过共识算法进行账本信息的广播和同步。

3.1.2　流通环节。主要节点是相关物流公司。接受了产品信息之后通过数字签名进行验证,通过验证后节点录入物流信息并上链,最后打上二维标识码,实现一物一码。

3.1.3　销售环节。主要节点是农资批发商、农资零售店。农资产品运输到各个地方,需要添加当前地方批发商或者零售店信息并进行上链,经过监管部门把关合格之后再打上标记。

3.1.4　监管者。主要节点是民地管理部门和市场监督部门。负责监管上述环节,审查合格后以数字签名方式检查各环节是否合格。

3.2　参与实体　每个参与实体都具有与智能合约的角色、关联和交互。共有 3 个参与实体,其作用概述如下:

3.2.1　生产商。农资生产公司是一个生产、流通、服务为一体的专业经营化肥、农药、种子、农机具等的大型企业集团。生产大量的农资产品,其中化肥业务主要为生产、销售各类氮肥、钾肥、磷肥、复合肥、有机肥及新型肥料;农药业务主要产品线为杀虫剂、杀菌剂、除草剂和微肥等;种子业务为生产流通粮食作物种子、瓜菜类作物种子、经济作物种子等。

3.2.2　运输商。农资运输商一般是由物流公司负责,具有运输农资产品的功能的从事客货运输生产服务的企业集团。物流公司根据不同的客户需求采取不同的运输途径,比如客运、火车和飞机,并将货物的运输信息记录下来,以便上传到区块链之中,方便消费者之后进行溯源。

3.2.3　销售商。销售商是指在能进行销售和服务的单位,有多层结构,可以分出二级经销商、一级经销商等,最终目的是为了获得经营利润。

结合传统农资溯源技术和区块链技术的特点,该研究设计了基于区块链的农资溯源系统模型,各节点单元为农资生产企业、农民生产企业、农资批发公司和监管部门,市场监督部门记录与产品相关的信息,将验证过的溯源信息数据最终上传至区块链上,并广播和同步至各个节点。

3.3　系统架构与模型　总体架构分为 4 层:用户层、系统层、存储层、智能合约层。由图 3 可知,智能合约层定义了一些事件流程,比如数据操作、资金周转、安全预警,当条件足够的时候会触发合约并执行,这些合约都是根据商业合同来进行编写的。存储层主要是使用分布式的方式将数据上传到区块之中进行存储,数据记录在默克尔树中进行哈希求值之后,另外再盖上时间戳,区块便开始产生。在联盟链里,只有部分节点才能进行访问,而公有链里所有节点都有权访问。存储层有 2 个部分,一般数据可以存储在数据库之中,重要的溯源信息则使用分布式存储在区块链里。这种方式既节省了空间,又确保了安全性。系统层使用的是传统农资溯源系统的框架模式,功能模块有企业管理、政府监督、和用户的相关服务等,面向的是用户和管理层还有监管者。用户层主

要是方便消费者和管理者进行可视化操作,使该系统更加实用。

该模型中,结合了区块链技术和加密技术,使用分布式存储和共识算法对农资溯源的安全提供保证。

图 3 基于区块链技术的农资交易溯源体系研究模型

Fig.3 Research on traceability system model of agricultural means transaction based on blockchain Technology

3.4 展示信息 按照市场的需求,尽量使得信息储存量最小化,难以篡改的信息和大型文件尽量上传至链,另外要界面简介,便于浏览。①生产环节的溯源信息。公司全称、商品全称、商品等级的信息、生产许可信息、质量检验信息、终端厂商地点、厂商内部终端生产线的定位、终端生产的时间、厂商指导价、联系人的姓名、联系人的电话等信息。②流通环节的溯源信息。各级销售商的全称、联系人的姓名、电话、交货时间、交货地址;售后服务商的全称、联系人的姓名、电话、地址。③商品的假冒信息。商品的"一物一码"二维码、其他防伪信息。④污染性的商品废弃处置信息。是否为需要回收处置的污染性商品、污染性商品的回收处置方式、污染性商品的回收处置情况。⑤用户反馈的信息。商品质量评价、使用效果评价、用户采购价格、投诉记录、其他必要信息。

4 系统测试

4.1 试验环境 该试验是在 ubuntu 16.04 64 位操作系统上进行的,系统配置为 CPU& 内存 1 核 2GiB。

4.2 试验过程 该试验对农资交易溯源上链时间进行检测,从溯源数据上链的响应时间来反映溯源系统的稳定性。该试验以不同的上链信息数据规模响应时间为评估要素,检测溯源数据上链的稳定性。

4.3 试验分析 由图 4 可知,频率上链相同,而溯源信息规模不同的情况下随着溯源信息规模越大,总响应时间不断增大,但平均时间并没有很明显的变化,在 3.0 ms 以下。由图 5 可知,随着溯源信息规模不断增大,TPS 保持在 30 上下波动。

通过试验可以看出,基于区块链的农资交易系统的响应时间在相同的请求频率下,在不同的溯源信息规模下面比较稳定,说明该系统具有稳定性,上链时间是毫秒级别,具有可拓展性。

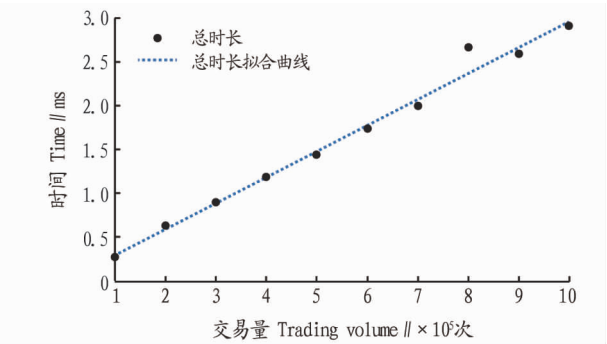

图 4 TPS 性能测试图

Fig.4 Test chart of uplink response time

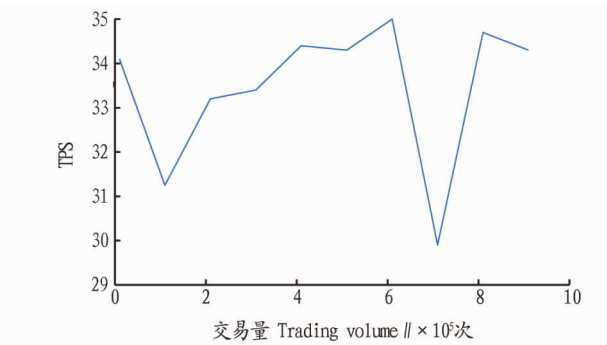

图 5 上链响应时间测试

Fig.5 Test of uplink response time

5 系统实现

基于上述架构和模型,设计并实现了一个基于区块链的农资交易溯源系统,该系统由前台和后台 2 部分组成,是面向农资消费者、生产者、市场监督者的农资可信品控溯源系统。

5.1 环境部署 该系统是在 Ubuntu 操作系统环境下,使用的是 Hyperledger Fabric 2.0 项目框架和 Docker、Git 等工具,后台是用 go 语言进行编写,前端使用 goweb 进行编写。

5.2 系统演示 系统有 2 个权限账户,一个是消费者,另一个是管理员。当消费者点击单号溯源时,就会跳转到查找界面,另外消费者可以点击"关于我们"和"帮助"来了解供应链企业信息和使用指南。管理员则可以点击"农资供应链管理"来进行信息管理。供应链环节分为 3 个流程:生产商、运输商、销售商,生产企业可以点击"生产商"进行添加信息功能,物流公司点击"运输商"进行运输信息上链,各级分销商可以点击"销售商"进行产品信息管理。消费者使用手机扫描产品包装上面的二维码时,就会跳转到系统的溯源信息界面,得到该产品在供应链各环节的溯源信息和人员信息和区块链信息(图 6)。后台负责显示区块链区块数目和 hash 等相关信息,网络层后台界面如图 7 所示。

6 结论

区块链技术的去中心化、不可篡改、分布式存储的天然特性,在农资溯源系统中具有很广阔前景。该研究分析了传统农资溯源系统存在的问题,提出了基于区块链的农资溯源系统的概念,对区块链溯源系统模型和系统架构进行了构建

图 6　产品信息溯源界面

Fig.6　Product information traceability interface

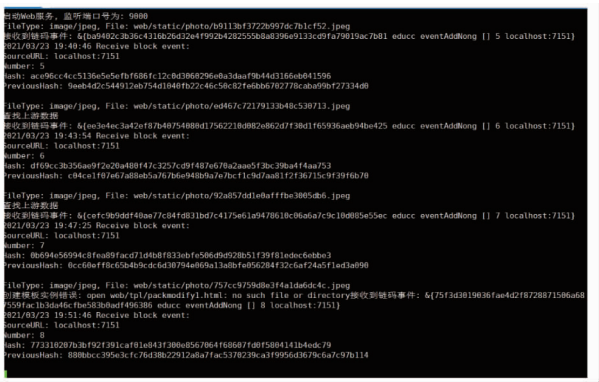

图 7　网络层后台界面

Fig.7　Network layer background interface

和分析,对智能合约进行设计使其满足农资产业链的实际需求,解决了传统农资溯源系统的信息易被篡改、信息不透明、存储安全性低等问题。在此基础上利用 HyperledgerFabric 平台实现了该区块链系统,该系统比传统溯源系统具有更高的安全性和可信性,它融合了区块链的特性,但是当前区块链技术并不成熟,上链速度和共识效率也有待提高。因此,如何提高区块链系统的性能和共识效率是后续研究中应着重解决的问题。

参考文献

[1] 陈义媛.中国农资市场变迁与农业资本化的隐性路径[J].开放时代,2018(3):95-111.

[2] 白红武,孙爱东,陈军,等.基于物联网的农产品质量安全溯源系统[J].江苏农业学报,2013,29(2):415-420.

[3] 黄庆,崔超远,乌云.应用于农资产品溯源服务系统的物联网技术分析[J].计算机系统应用,2013,22(1):44-47.

[4] 郑开涛,刘世洪.农产品质量安全溯源多边平台的研究与设计[J].中国农业科技导报,2017,19(12):52-58.

[5] 吴晓彤.基于区块链的农产品可信溯源系统研究与实现[D].泰安:山东农业大学,2020.

[6] EKWUE E I,STONE R J.Organic matter effects on the strength properties of compacted agricultural soils[J].Transactions of the ASAE,1995,38(2):357-365.

[7] 林有新,罗伦华.深化改革 强化联合 服务"三农":简述农资流通主渠道的困境与对策[J].农资科技,1997(4):37-39.

[8] 农资质量安全追溯平台上线[J].蔬菜,2017(10):63.

[9] 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.

[10] 陈固.区块链技术应用前景广阔[J].数字通信世界,2018(S1):64.

[11] ZHENG Z B,XIE S A,DAI H N,et al.An overview of blockchain technology:Architecture,consensus,and future trends[C]//2017 IEEE international congress on big data (BigData congress).Honolulu,HI,USA:IEEE,2017:557-564.

[12] YI W L,HUANG X M,YIN H,et al.Blockchain-based approach to achieve credible traceability of agricultural product transactions[J].Journal of physics:Conference series,2021,1864(1):1-4.

[13] PRASHAR D,JHA N,JHA S,et al.Blockchain-based traceability and visibility for agricultural products:A decentralized way of ensuring food safety in india[J].Sustainability,2020,12(8):1-20.

[14] KARAMITSOS I,PAPADAKI M,AL BARGHUTHI N B.Design of the blockchain smart contract:A use case for real estate[J].Journal of information security,2018,9(3):177-190.

[15] 屈志毅,苏文洲,赵玲.一种基于信息分散算法的分布式数据存储方案[J].计算机应用,2006,26(5):1102-1105.

[16] 杨茂,文斌,卢德全.基于区块链的食品溯源研究与应用[J].计算机科学与应用,2019(3):580-587.

[17] 曹俭,林亮,李云,等.区块链研究综述[J].重庆邮电大学学报(自然科学版),2020,32(1):1-14.

[18] 谭春桥,杨慧娟,易文桃.基于纳什谈判的共享经济区块链网络 PoS 共识传播博弈分析[J].控制与决策,2022,37(1):219-229.

[19] 黄嘉成,许新华,王世纯.委托权益证明共识机制的改进方案[J].计算机应用,2019,39(7):2162-2167.

[20] 曾景峰,万梅芬.物联网技术在农产品追溯中的应用[J].物流技术,2014,33(19):449-450,456.

[21] SALAH K,NIZAMUDDIN N,JAYARAMAN R,et al.Blockchain-based soybean traceability in agricultural supply chain[J].IEEE access,2019,7:73295-73305.

[22] OPARA L U.Engineering and technological outlook on traceability of agricultural production and products[J].Agricultural engineering international,2002(4):1-13.

[23] ZHAO Y B,CAO N.Research on traceability of agricultural products based on internet of things[C]//2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC).Guangzhou,China:IEEE,2017:414-417.

[24] 莫璋红,吴丽丽,阮建明,等.我国食品安全可追溯系统及在乳制品中的应用[J].安徽农业科学,2017,45(12):203-206.

[25] WANT R.An introduction to RFID technology[J].IEEE pervasive computing,2006,5(1):25-33.

[26] ANGELES R.RFID technologies:Supply-chain applications and implementation issues[J].Information systems management,2005,22(1):51-65.

[27] TIWARI S.An introduction to QR code technology[C]//2016 international conference on information technology (ICIT).Bhubaneswar,India:IEEE,2016:39-44.