doi:10.6041/j.issn.1000-1298.2021.01.001

农产品供应链区块链追溯技术研究进展与展望

孙传恒[1,2]　于华竟[1,2]　徐大明[1,2]　邢　斌[1,2]　杨信廷[1,2]
(1. 国家农业信息化工程技术研究中心，北京 100097；2. 农产品质量安全追溯技术及应用国家工程实验室，北京 100097)

摘要：农产品供应链具有链条长、生产分散、信息多源异构等特点，极易造成供应链上下游信息断链和不透明。传统追溯数据存储于各节点企业，在供应链上下游数据传递过程中存在协作信任度低、真实性差等问题，造成消费者对追溯信息的真实性产生信任危机。区块链追溯系统通过建立多方参与、共同维护的分布式数据库，并利用密码学和共识机制建立信任关系，具有数据无法篡改、共享可信度高等优势，近年来成为国内外研究的热点。本文系统总结了国内外农产品区块链追溯系统的研究进展，从区块链追溯链上链下数据协同、区块链追溯共识机制和区块链追溯数据隐私保护等方面详细分析了区块链追溯关键技术的研究进展；对区块链追溯技术的未来发展进行了展望，指出区块链规模化应用后多链和跨链技术将成为发展趋势，区块链技术与物联网、人工智能、大数据等新一代信息技术的深度融合将推动农产品供应链追溯进入新的发展阶段。

关键词：农产品；供应链；区块链；追溯；密码学；共识机制
中图分类号：TP309.2；TS201.6　**文献标识码**：A　**文章编号**：1000-1298(2021)01-0001-13　**OSID**：

Review and Prospect of Agri-products Supply Chain Traceability Based on Blockchain Technology

SUN Chuanheng[1,2]　YU Huajing[1,2]　XU Daming[1,2]　XING Bin[1,2]　YANG Xinting[1,2]
(1. *National Engineering Research Center for Information Technology in Agriculture*, *Beijing* 100097, *China*
2. *National Engineering Laboratory for Agri-product Quality Traceability*, *Beijing* 100097, *China*)

Abstract: The agricultural product supply chain has the characteristics of long chain, decentralized production, and heterogeneous information from multiple sources, which can easily lead to disconnection and opacity of upstream and downstream information in the supply chain. Traditional traceability data is stored in each node enterprise, and there are problems such as low collaboration trust and poor authenticity in the upstream and downstream data transmission process of the supply chain, which causes consumers to have a trust crisis in the authenticity of traceability information. The blockchain traceability system establishes a distributed database with multi-party participation and joint maintenance, and uses cryptography and consensus mechanisms to establish a trust relationship. It has the advantages of inability to tamper with data and high sharing credibility. In recent years, it has become a research hotspot at home and abroad. The research progress of blockchain traceability systems for agricultural products at home and abroad was systematically summarized, and the blocks were analyzed in detail: blockchain traceability on-chain and off-chain data collaboration, blockchain traceability consensus mechanism, and blockchain traceability data privacy protection. Finally, after the large-scale application of the blockchain, multi-chain and cross-chain technology would become the development trend, and it was predicted that the blockchain technology would be deeply integrated with the new generation of information technology such as the internet of things, artificial intelligence and big data, which was going to promote the blockchain traceability supply chain to enter a new stage of development.

Key words: agricultural products; supply chain; blockchain; traceability; cryptography; consensus mechanism

收稿日期：2020-10-20　修回日期：2020-11-11
基金项目：国家自然科学基金面上项目(31871525)和北京市自然科学基金面上项目(4182023)
作者简介：孙传恒(1978—)，男，研究员，博士，主要从事农产品追溯技术研究，E-mail：sunch@nercita.org.cn
通信作者：杨信廷(1974—)，男，研究员，博士，主要从事农产品智慧供应链研究，E-mail：yangxt@nercita.org.cn

0 引言

近年来,农兽药残留超标等农产品质量安全事件频发,不仅危及人们的身体健康,同时也对农产品出口贸易造成不利的影响,因此成为社会关注的热点[1-2],农产品追溯系统成为保障农产品安全的重要手段。农产品追溯系统能够记录、存储供应链从生产到销售的数据信息,一旦发生农产品质量安全问题,系统能够快速追溯产品来源,并且定位责任主体,及时召回有问题批次的产品[3]。

目前,追溯系统的研究主要集中在射频识别[4]、二维码[5]、无线传感网络[6]等物联网技术对追溯信息的采集方面,但国内农产品供应链具有链条长、生产分散、信息多源异构等特点[7],供应链上下游主体由于复杂的利益博弈关系,造成各节点间信息不对称、信任成本较高等问题,影响了整体追溯效率。同时,传统追溯系统存在无法将供应链各环节的追溯信息进行准确关联、由企业中心数据库自主管理供应链数据等问题,导致追溯信息不精确、不完整[8],产生纠纷时举证困难、责任难以明确[9]。因此,传统追溯技术无法完全解决我国农产品供应链追溯中存在的问题,探索有效的技术方案成为国内外研究的热点。

区块链技术基于分布式存储、点对点传输、共识机制、加密算法等关键技术,具有去中心化、数据不可篡改、可追溯、高可用等特点[10],能够有效解决供应链上下游数据在传递过程中的信任问题,从而构建与追溯需求吻合的可信交易环境。区块链技术与农产品追溯相结合,能做到分散资源集中管理、集中资源分散服务,为解决目前传统追溯体系存在的问题提供了技术支撑[11]。近年来国内外学者从不同角度研究了区块链技术在供应链追溯中的应用,如KORPELA 等[12]、KSHETRI[13]和 MEZQUITA 等[14]从交易管理方面探讨了区块链技术在供应链上的应用,KAMILARIS 等[15]和 FRANCISCO 等[16]从供应链数据透明管理方面探讨了区块链追溯的应用,AZZI 等[17]和 LU 等[18]从区块链架构方面讨论了区块链技术在供应链上的应用,BUMBLAUSKAS 等[19]和 ZHAO 等[20]从系统集成方面研究了区块链在果蔬农产品供应链上的应用,KAMATH[21]结合具体案例认为,区块链在沃尔玛食品供应链中具有快速可信追溯的优势。在整个供应链或部分生产和使用环节自动获取产品历史、应用情况或所处位置等信息之间相互关联或相互作用的区块链农产品追溯系统成为国内外研究的热点和方向[22]。

本文综合分析国内外区块链追溯技术研究进展,在对比传统追溯技术和区块链追溯技术基础上,分析区块链追溯的概念;并从区块链追溯链上链下数据协同、区块链追溯共识机制和区块链追溯数据隐私保护等方面阐述区块链在农产品供应链上的关键技术研究进展,最后从多链和跨链技术以及与新一代信息技术融合方面展望区块链追溯的发展趋势。

1 传统追溯技术

追溯是指通过记录或标识,追踪和追溯客体的历史、应用情况或所处位置的活动,追溯系统指基于追溯码、文件记录、相关软硬件设备和通信网络,实现现代信息化管理并可获取产品追溯过程相关数据的集成[23]。农产品供应链追溯重点跟踪记录农产品在生产、加工、运输、销售等环节的数据,实现“从农田到餐桌”的全环节监管[24]。表 1 列出了国内外在水产品、农产品、果蔬等大型生鲜农产品领域建立的典型追溯系统[25-26]。

表 1 农产品传统追溯系统

Tab. 1 Agricultural products traditional traceability system

追溯主体	追溯环节	数据获取	数据存储	数据监管	数据标识
水产品[27]	加工环节、运输环节、商户和质检环节	企业录入	追溯中心数据库	监管部门	二维码和条形码
蔬菜[28]	生产管理环节、数据上传环节、编码环节、流通环节	掌上计算机控制采集、人工录入、数据库导入	企业数据库和追溯中心数据库	企业监管部门	二维码
脐橙[29]	果园信息管理环节、加工环节、仓储环节、运输环节、营销环节	企业录入	追溯中心数据库	企业监管部门	RFID(Radio frequency identification)条码
农产品[30]	种植环节、采收环节、加工环节、销售环节	终端设备采集	企业数据库、产品数据库、生产档案数据库	监管部门	二维码

从表 1 可看出,传统农产品追溯系统存在人工干预数据录入、依赖第三方机构监管数据安全、数据存储在企业本地数据库等问题,极易引起数据传递和共享过程中的篡改和泄露危机[31]。

2 区块链追溯

2.1 区块链简介

区块链是多方参与共同维护的持续增长的分布

式数据库[32-33]，基于分布式网络、密码学和共识机制建立信任关系，通过智能合约构建价值互联网。区块链的本质是共享账本[34]，通过开发分布式平台解决主体协作、信息误传、缺乏监管的问题；基于全网节点的计算、存储和网络共享模型，提供大数据共享和证据保存；通过零知识证明[35]和安全多方计算，实现数据的验证而不披露。区块链网络架构下所有节点互联互通、对等通信，共同查询、记录、维护账本数据，打破信息孤岛，扩展网络化运行的边界，实现区块链网络的去中心化[36]。

区块结构由区块头和区块体组成(见图 1)。区块头存储上一区块的哈希值，实现链上数据的可信追溯，在长链中修改任一区块的数据将导致本区块哈希无效，从而引起断链，需要消耗巨大算力重新计算本区块和所有后续区块哈希值；根据区块头存储的 Merkle 根能够快速验证交易数据的篡改，以上两种机制保证了区块数据一经验证写入便不可篡改[37]。区块体则包含了经过验证的、块创建过程中发生价值交换的所有追溯记录，具体追溯记录字段因节点不同而存在差异。

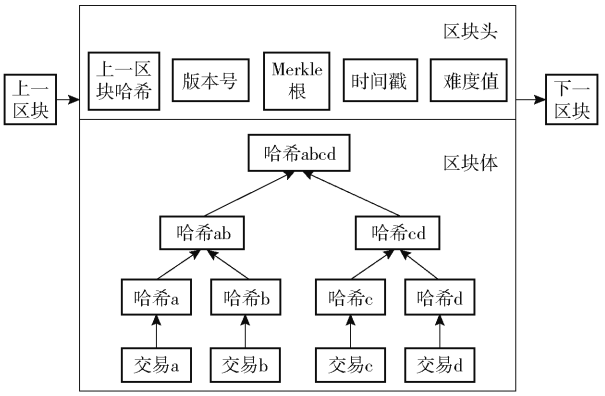

图 1　区块结构示意图

Fig. 1　Structure diagram of block

2.2　区块链分类

根据节点参与方式，区块链可划分为公有链(Public Blockchain)[38]、私有链(Private Blockchain)[39]和联盟链(Consortium Blockchain)[40]。根据节点参与权限，区块链可划分为许可链(Permissioned Blockchain)[41]和非许可链(Permissionless Blockchain)[42]。表 2 分析了不同类型的区块链在节点参与、记账权、读写权限、激励方式以及网络特征等方面的特点。

表 2　区块链类型

Tab. 2　Type of blockchain

链类型	公有链	私有链	联盟链
参与节点	参与者为所有人	参与者为个人或组织	参与者为联盟成员
记账权	根据共识机制争取记账权	个人或组织内部自定义记账权	联盟成员协商确认后进行记账
读写权限	对参与节点读写无限制	写入权限归内部控制，读取权限视需求开放	通过授权，节点可读写
激励方式	需要	不需要	视业务需求自定义激励方式
网络特征	去中心化、网络规模较大，吞吐量较低	弱中心化、网络规模较小，吞吐量较高	多中心化、网络规模较小，吞吐量较高
数据存储	所有节点	弱中心化机构节点	多中心节点
应用领域	交易数据公开，主要应用于虚拟货币领域	交易数据不公开，主要应用于审计、银行领域	通道隔离交易数据，主要应用于跨行业、跨生态的协作

2.3　区块链追溯技术

区块链追溯系统是在追溯系统中引入区块链技术，实现农产品生产信息、加工信息、运输信息以及销售信息的数据一旦验证通过写入区块账本就无法修改，保证数据的真实、透明、可靠[43]。表 3 列出国内外主流组织和权威学者对区块链追溯的定义。从中可以看出，农产品区块链追溯目的是实现农产品全生命周期跟踪追溯，构架农产品供应链间的沟通桥梁，提升信息的透明度和真实性，在追溯平台信任得到了良好的维护。

2.4　联盟链追溯技术

我国农产品供应链追溯参与主体多、链条复杂，产业链呈现“两头小中间大”特征，通过联盟链多中心化网络结构平衡多参与主体问题，有效提高农业生产活动中各参与主体的协作效率，构建透明、真实、可信的农产品追溯体系。表 4 列出部分农产品供应链追溯体系，从表 4 中能够看出基于联盟链开展区块链追溯研究已成为国内外热点和共识。

3　区块链追溯关键技术研究进展

基于联盟链的农产品供应链追溯系统利用各种物联网采集和保存方式，获得农产品在生产、加工、运输以及销售过程中的关键数据，同时利用智能合约自动执行交易条款，基于非对称加密和数字签名保证交易数据的唯一性和安全性，通过多通道的事务隔离性提供隐私保护，确保了信息流、资金流、物流和商流的可靠流转，在离散程度高、链条长、参与主体多的农产品供应链中实现多组织高效协作、资

表 3 区块链追溯定义

Tab. 3 Concepts of blockchain traceability

组织或学者	文献名称或部门	区块链追溯定义
工业和信息化部信息中心	中国区块链产业白皮书[44]	中国食品区块链追溯基于区块链技术,对产品种植、生产、加工、包装、运输和销售等全流程进行追溯
可信区块链推进计划溯源应用项目组	区块链追溯应用白皮书[45]	物品或信息在生产、流通以及传输过程中,利用采集和留存方式,获得物品或信息的关键数据,将数据按照一定的格式存储在区块链上,通过查询相关数据实现对物品及信息的追溯
BETTIN-DIAZ 等	Methodological approach to the definition of a blockchain system for the food industry supply chain traceability[46]	区块链追溯是从生产到销售全环节数据写入区块链网络,全网节点共同维护、备份数据,通过区块链结构实现数据追溯
腾讯研究院	2019 腾讯区块链方案白皮书[47]	区块链追溯通过区块链记录供应链上的全流程信息,实现产品材料、原料和产品的起源和历史等信息的检索及追踪,提升供应链上信息的透明度和真实性
杨信廷等	基于区块链的农产品追溯系统信息存储模型与查询方法[48]	区块链追溯是在追溯系统中引入区块链技术,利用区块链的去中心化、不可篡改、可追溯等特性,保证农产品追溯系统的追溯信息真实透明

表 4 区块链追溯系统

Tab. 4 Blockchain traceability system

标题	简介	应用	平台
A simulated organic vegetable production and marketing environment by using ethereum[49]	基于以太坊平台记录有机蔬菜从生产到销售全环节数据,提供数据的可信追溯	有机蔬菜	以太坊(Ethereum)
Blockchain-based soybean traceability in agricultural supply chain[50]	基于以太坊和智能合约执行交易,保证全球贸易中大豆供应链的可追溯性	大豆	以太坊(Ethereum)
Food safety traceability system based on blockchain and EPCIS[51]	基于以太坊平台构建可信和可追溯的供应链系统,保证食品在生产、加工、运输和零售等环节数据的安全问题	食品	以太坊(Ethereum)
An agri-product traceability system based on IoT and blockchain technology[52]	基于联盟链和物联网设备搭建可靠、可信和可扩展的农产品追溯系统,保障食品质量安全	食品质量	联盟链(Consortium Blockchain)
A novel visual analysis method of food safety risk traceability based on blockchain[53]	基于 Hyperledger 构建可视化信息存储平台,解决传统食品追溯系统存在的问题	追溯信息存储	Hyperledger
A secure fish farm platform based on blockchain for agriculture data integrity[54]	基于 Hyperledger fabric 架构为养鱼场系统提供数据无法篡改的数据存储空间	追溯信息存储	Hyperledger fabric
Blockchain-based safety management system for the grain supply chain[55]	基于 Hyperledger fabric 构建可追溯系统,保证生命周期长、链条复杂的谷物供应链食品质量和安全	食品质量和安全	Hyperledger fabric
FastFabric: scaling Hyperledger fabric to 20 000 transactions per second[56]	设计一个即插即用的现代许可区块链系统 FastFabric,事务吞吐量从 3 000 个/s 增至 20 000 个/s	提高联盟链吞吐量	Hyperledger fabric

源共识共享共治的智能化配置,大幅降低农产品供应链成本。区块链技术涉及到组网建链、数据协同、共识算法、智能合约、隐私保护和模式标准等系列技术,限于篇幅,本文重点从区块链追溯链上链下数据协同、区块链追溯共识机制和区块链追溯隐私保护方面分析区块链追溯关键技术的研究进展。

3.1 区块链追溯链上链下数据协同技术

国内联盟区块链追溯的发展重点方向是链上链下的数据协同[57],在区块链追溯系统中链上需要链下的信息系统扩展计算和存储能力,链下的信息系统需要和链上对接实现异构信息共享解决信息孤岛问题[58]。区块链追溯链上通过哈希函数的单向加密和不可碰撞性保证链上信息完整性,但却无法解决链下虚假数据或真实数据上链过程的真实性问题[59],为实现大批统一的区块链应用落地,区块链链上链下数据协同能力成为目前研究热点。

区块链追溯系统通过第三方机制下的预言机、状态通道等实现链上对链下数据的可信访问。预言机是一种通过签名引入外部世界状态信息的可信任的实体,响应链上智能合约提出的数据交互需求,通过单向的数字代理以加密的方式将不经过计算就能够证明的外界数据提交给智能合约进行加工处理实现数据协同[60]。如 WANG 等[61]、ADLER 等[62]和 LO 等[63]分析预言机将外部数据带入区块链的数据协同问题。状态通道[64-65]对区块链进行初始化、终止化或净额结算,把链上的数据操作转移到链下的状态通道中加工处理后上链计算结果。状态通道能

够显著提高链上交易效率、降低数据协同成本，并且在数据协同方面具有天然的安全性优势[66]。表 5 列出将数据在链上链下分类存放以实现区块链追溯链上链下的数据协同。

表 5　区块链追溯链上链下数据协同技术

Tab. 5　Traceability data cooperation based on blockchain technology

学者	文献名称	数据协同
宋俊典等	基于区块链的数据治理协同方法[67]	链上存储行业标准库负责存储读取数据，链下通过身份认证模块、权限管理模块、监督管理模块等验证数据
SHEN 等	Blockchain-based incentives for secure and collaborative data sharing in multiple clouds[68]	链上通过智能合约调取链下存储在私有或公有云平台的数据
杨信廷等	基于区块链的农产品追溯系统信息存储模型与查询方法[48]	链上存储数据密文，链下存储追溯数据

3.2　区块链追溯共识机制

区块链分布式网络处理容错的核心是共识机制，全网节点在预设规则下与其它节点交互达成对数据、行为或流程的一致，实现交易的不可变、全局一致的注册[69]。公有链常用工作量证明机制 PoW（Proof of work）、权益证明机制 PoS（Proof of stake）和委托权益证明机制 DPoS（Delegated proof of stake）等共识机制；联盟链常用实用拜占庭容错算法 PBFT（Practical byzantine fault tolerance）、Kafka 等共识机制；私有链中常用 Raft 共识机制。表 6 对不同区块链网络中的共识算法进行了分析对比。

工作量证明机制（PoW）通过结果认证证明完成了相应的数学计算，具有完全去中心化的优点，在以工作量证明机制为共识的网络中，节点可以自由进出。权益证明机制（PoS）根据节点持有代币的比例和时间，依据算法按币龄权重等比降低寻找随机数的难度值。委托权益证明机制（DPoS）一方面集成了权益证明机制的币龄优势，另一方面由持币人选举公证人节点参与验证、记账，对去中心化做出了一定妥协。张利等[75]提出的基于区块链的农产品追溯系统中节点通过工作量证明共识机制竞争记账权。LENG 等[76]考虑农业经营中的激励权重问题，在权益证明机制共识机制的基础上，提出一种考虑农企权重的一致性共识算法。梁昊等[77]设计的农产品信息区块链技术架构使用委托权益证明机制共识机制通过节点表决认可农

表 6　区块链追溯共识算法

Tab. 6　Consensus algorithm of blockchain traceability

共识算法	记账权	容错性	优势	劣势	应用场景
PoW[70]	根据难度值消耗全网算力，经过大量数学计算得出合理的区块哈希值竞争记账权	存在 51% 攻击，允许全网 50% 节点出错	共识机制高、节点动态加入或退出	资源消耗大、可监管性弱、共识周期长	比特币（BitCoin）、以太坊前 3 阶段
PoS[71]	根据币龄等比例降低计算哈希值的难度值竞争记账权	根据币龄获取记账权，记账成功币龄清空，节点作恶成本较高	共识时间有效缩短、资源消耗降低	持币吃息影响币流动、根据币龄结余引起首富账户支配记账权	以太坊的第 4 个阶段
DPoS[72]	无序竞争，由持币者选举代理节点进行验证和记账	代理节点出现算力不稳定、作恶操作，持币人可随时通过投票更换	验证和记账的节点少、秒级共识、共识公平民主	共识机制依赖代币	EOS 币、BTS 币
PBFT[73]	无需竞争，在大于 $3f+1$ 的全网节点中选取主节点，由主节点进行验证、记账	支持全网存在少于三分之一的恶意节点	较少节点情况下性能较高、分叉概率低	系统节点增多共识效率下降且存在主节点出错问题	在 Hyperledger fabric 中设计成 PBFT 共识可插拔模组、央行数字货币
Kafka[72]	无需竞争，Kafka 集群的排序服务节点根据交易请求分发到不同分区处理	集群中客户端和服务器端通过 SSL（Secure sockets layer）数据加密、通过 SASL（Simple authentication and security layer）用户认证	网络共识由 Kafka 集群实现，具有较高的吞吐量	新增 Kafka 集群，增加系统开销	在 Hyperledger fabric 中设计成 Kafka 可插拔模组
Raft[74]	无需竞争，由全网节点选取具有完全权力管理的主节点进行验证、记账、广播结果	主节点失联后，候选节点重新选举主节点，失联期间，旧主节点所有操作回滚撤销，恢复连接后成为候选节点	算法容易部署实现且易于理解、共识高效	只能容纳故障节点，不能容纳作恶节点，不具备拜占庭容错特性	在 Hyperledger fabric 和 FISCO BCOS 的区块链系统中设计为可插拔的 Raft 模组

产品信息的准确性。

实用拜占庭容错算法(PBFT)不仅考虑节点宕机且支持节点主动作恶情况,算法分为预准备、准备、确认 3 阶段,保证全网三分之一节点的容错性,在划分主节点和副本节点上,袁勇等[78]提出一种基于监督模型的共识算法 MBFT(Multisignature byzantine fault tolerance)解决主节点出错问题,任守纲等[79]在农作物全产业链追溯信息平台中提出一种信誉监督机制拜占庭容错共识算法 CSBFT(Credit-supervisor byzantine fault tolerance)解决副本节点身份确认问题。王志铧等[80]使用 Hyperledger fabric 平台设计的生姜区块链追溯系统采用 Kafka 共识机制同步数据,实现数据存储安全、追溯数据清晰。未来针对不同品类的农产品供应链应用场景,开发适配不同应用模式的共识算法将是重要的研究方向之一。

3.3 区块链追溯数据隐私保护技术

区块链基于对称加密算法、非对称加密算法、哈希算法保证数据完整性、隐私性和有效交易凭证[81],并使用数字签名保障交易安全,尤其以椭圆曲线加密算法生成公私钥对和椭圆曲线数字签名算法保障交易不可抵赖为代表,并通过零知识证明和多方安全计算实现数据的安全验证[82]。表 7 对比分析了隐私保护加强技术。

表 7 隐私保护加密技术

Tab.7 Cryptography technology of blockchain traceability

加密技术	算法简介	优势	代表
对称加密	采用单密钥的方式进行加密、解密	计算量小且加密效率高	DES(Dataencryption standard)、3DES、AES(Advanced encryption standard)
非对称加密	采用公私密钥对加密和解密,公钥加密的数据,只有对应的私钥可以解开,反之亦然	计算量大且不易破解	RSA、椭圆曲线加密算法 ECC(Error correcting code)
Hash 算法	对任何大小的输入计算相对唯一的输出,即使对输入的最小更改也将导致完全不同的输出	数据快速验证且密文不可逆转	信息摘要算法 MD5(Message-Digest algorithm)、安全散列算法 SHA-256(Secutiry hash algorithm)
数字签名	使用非对称加密算法让信息的发送者使用私钥加密别人无法伪造的密文	保障交易安全,生成抗抵赖性的交易凭证	椭圆曲线数字签名
零知识证明	证明者能够在不向验证者提供信息本身内容的情况下,使验证者相信某个论断是真实可信	验证者在相信示证者的同时不会获取有关被证明论断的任何知识	验证而不披露数据
安全多方计算	在分布式网络中,多个参与实体各自持有秘密输入,各方希望共同完成对函数的计算,且每个参与实体除计算结果外均不能得到其他参与实体的任何输入信息	在无可信第三方情况下,安全地进行多方协同计算	输入保密的情况下得到输出结果

根据表 7 的对比分析可知,对称加密简单快捷、密钥较短但破译困难,在对称加密方面,于合龙等[11]设计的基于区块链的水稻供应链追溯系统采用对称加密 AES 中的密码分组链接 CBC(Cipher block chaining)模式加密隐私数据,并使用椭圆曲线算法 ECC(Elliptic curve cryptography)加密密钥实现密钥授权。李文勇等[83]改进对称加密算法 AES,实现了一种基于嵌入式平台的可直接加密十进制数据的农产品追溯码加密算法,设计基于地理坐标编码方式的农产品追溯码。

非对称加密采用公私密钥对保证数据隐私。在非对称加密方面,马腾等[84]结合 RSA 加密算法和 ASCⅡ码设计农产品原产地可信追溯系统。张旭凤等[85]采用 RSA 加密算法设计基于区块链技术的农产品物流信息系统。王乃洲等[86]通过 RSA 加密算法和共识算法保证基于区块链的用户身份认证信息的安全性。基于非对称加密的数字签名能够保证交易凭证和识别交易发起者身份,徐蜜雪等[87]针对区块链安全问题设计的拟态区块链使用一种异构签名算法,采用 3 种签名算法代替单一的签名算法签名消息应对安全威胁。

Hash 函数可识别源数据的任何更改且具有单向不可还原特点,在哈希算法方面,李宣等[88]基于区块链和物联网设计的双区块链防伪追溯系统,基于私有链存储交易数据,交易明文经过 Hash 函数加密后的密文上传到联盟链。杨信廷等[48]设计的农产品区块链追溯系统信息存储模型将追溯明文信息存储在各节点本地数据库,上传 MD5 哈希算法加密数据的密文到区块链。

零知识证明和安全多方计算强调输入数据的保密性,弥补区块链重视计算的可验证性而忽略数据验证性的问题。李佳潞[89]在基于区块链的粮食供

应链追溯方案研究中，设计基于零知识证明算法的共识机制用以验证链上隐私数据的一致性和完整性。黄建华等[90]在利用区块链构建公平的安全多方计算中，基于区块链智能合约构造惩罚机制提出公平的安全多方协议。

从上面分析可以看出，未来基于上述数据隐私保护技术开发可插拔的加密算法，将是农产品供应链追溯的重要方向，同时在应用方面结合权限控制体系和证书认证体系管理多组织间信息传递或共享，将权限管理紧密结合供应链追溯业务场景，将加速促进区块链追溯的应用落地。

4　区块链追溯应用

在区块链追溯应用实践方面，国内外商业公司进行了积极的探索。比较典型的是蚂蚁集团研发的蚂蚁链、京东集团研发的智臻链以及江苏中南建设集团股份有限公司联合黑龙江北大荒农业股份有限公司设计构建的区块链大农场。其中，蚂蚁链通过将网络准入权限与支付宝绑定，实现一键式快速部署，已应用于奶粉、大米、红酒、蜂蜜等全球 30 亿件商品的原产地或境外溯源保真，溯源产地覆盖 120 个国家，支持 14 万类商品，解决溯源信息的真实性问题[91]，智臻链已有超 13 亿条上链数据，700 余家合作品牌商，5 万以上 SKU（Stock keeping unit）入驻，逾 280 万次售后用户访问查询，解决价值网络中信息流转不畅、信息缺乏透明度、信息不对称等问题[92]，区块链大农场应用于北大荒高度组织化的农场种植模式，有 9 种物联网数据采集标准，112 个电子表单，63 个农作物种植规范，覆盖北大荒近百万公顷土地，解决北大荒自然资源向数字资产可信转移的问题[93]。

目前区块链大规模商业化应用仍处于前期阶段，阻碍其大规模应用的原因复杂，其中区块链通用底层平台欠缺[94]、基础设施不健全且性能不完善[95]、兼容性不足，导致绝大部分与区块链结合的追溯的商业场景仍然处于探索期[96]。另一方面，技术发展初期的缺陷暂时无法解决，如区块链单链存储结构[97]难以负载海量数据存储压力，多链间数据隔离[98]难以做到数据的动态扩展，都限制区块链追溯网络进一步扩大。同时联盟链网络缺乏统一的行业标准，难以构建联盟链统一生态网络架构[99]。

在解决区块链追溯大规模应用方面，可以从技术和经济两方面协同推进。技术方面需要开发区块链追溯行业通用支撑服务平台[100]，降低企业使用门槛，支撑区块链追溯应用快速落地，另一方面针对供应链区块链追溯链条长、多主体离散程度高等问题研究区块链追溯共识算法，提升共识算法效率和区块链性能，同时解决突破多链、跨链、链上链下数据协同机制，进一步扩大追溯生态网络[101]。经济方面充分利用区块链的智能合约和共识算法，解决供应链追溯跨主体多方协助合理的分配机制和激励机制[102]，实现追溯数据存储在网络中，让追溯数字经济在价值互联网中可靠传递，解决价值传递过程中存在的基础资产真实性低、资产流通成本高、流动性差等问题。

5　区块链追溯技术展望

5.1　区块链技术发展方向

5.1.1　多链技术

农产品区块链追溯规模化应用后，受到共识速度的限制，节点的执行性能难以线性扩展，链上交易在区块链单链账本中串行处理，难以获得接近中心化系统的性能表现。未来区块链的发展趋势将改变单链主导，实现多条同构链或异构链并存的区块链新生态系统，解决供应链中存在的上下游博弈问题，实现多组织的信息对称并降低上下游组织信任成本。刘家稷等[103]设计使用公有链和私有链构建追溯系统，使用私有链存储企业产品信息，使用公有链保证链上数据的可验证和不可篡改，实现数据的可靠存储和企业自管理隐私数据。LENG 等[76]提出的基于双区块链的农产品供应链系统选用公有链存储公共服务平台上企业用户信息，在私有链上存储企业隐私数据和交易数据。DING 等[104]提出了双链的追溯许可链共识机制，主层部署联盟链用来追溯信息查询共享，辅助层部署私有链存储追溯信息，在保证追溯链私密性的同时，系统也随着参与节点的增加保持高效的运行效率。

5.1.2　跨链技术

区块链在农产品供应链追溯具体的应用场景中需要适应多样化的业务需求，方便跨企业、跨生态业务数据的共享。在大批统一的区块链应用场景下，采用不同的通信协议、编程语言、共识机制和隐私措施搭建的相对独立的、缺乏统一的互联互通机制的异构链难以做到价值互通、适应不同的场景需求，因此，异构链间实现跨链的价值传递将是区块链追溯生态健康发展的必然要求。跨链[105-108]通过中间件实现异构链的互联互通，实现账本的跨链互操作，为追溯行业跨生态、跨行业的多维协作解决信息孤岛问题，从追溯异构链“孤岛”发展成为异构链“网络”。

5.2 与新一代信息技术融合助力追溯产业

以物联网、大数据、人工智能、云计算和 5G 为代表的新一代信息技术和区块链的深度融合为农产品供应链追溯行业提供了巨大的潜在空间[109]。新一轮科技革命中各有侧重并相互关联,物联网负责收集数据,全网海量数据汇集存储在链下云端形成追溯大数据,云计算完成数据的高效查询操作,大数据为人工智能提供训练数据集不断优化模型参数,构建辅助决策生产模型改进供应链上下游智能决策;区块链作为信任桥梁稳定涉及数据操作的信任机制,保证数据传递、共享的稳定可靠[110]。

5.2.1 区块链 + 物联网

区块链是构建物联网真正分散、无信任和安全环境的缺失环节,通过区块链的分布式网络、不可篡改和可追溯的优势为物联网的安全应用提供媒介[111]。区块链 + 物联网实现物物之间信用的无风险、无杠杆的高效率传递,链上实现资金流、物流、信息流三流合一[112],在物联网万物互联的基础上保证万物可信,实现物理世界和数字世界的映射,保证上链信息的真实性和完整性,进一步助力智慧供应链追溯发展。表 8 列出了部分区块链 + 物联网模式在追溯方面的应用。

表 8 基于区块链和物联网的追溯技术

Tab. 8 Traceability based on blockchain and IoT

物联网设备	简介	文献序号
RFID	在生产、加工、运输、销售全环节给产品添加 RFID 标签保存产品信息,产品信息密文存储在联盟链以便数据验证	[113]
RFID	提出基于以太坊、智能合约和 RFID 标签的国际商业食品追溯系统,使用 RFID 标签记录食品标识符,通过无线通信设备读取区域内食品的唯一标识符发送到数据中心进行上链处理	[114]
RFID	在贴有 RFID 标签物品生产、加工、仓储、运输、销售等多环节建立区块链账本,建立起 RFID 大数据的追溯全程链式路径	[115 - 116]
Lora	通过 Lora 设备减少人工干预数据;区块链验证存储数据;智能合同脚本实现自动报警;实现可信、自组织的和开放透明的智慧农产品追溯系统	[117]
物联网传感器	基于以太坊或 Hyperledger sawtooth 等实施集成物联网传感器设备,通过 IoT 设备记录农产品供应链中有价值的信息并将这些数据直接上链存证	[118]

在区块链农产品追溯系统中使用 RFID 标签、无线传感器 WSN(Wireless sensor network)、北斗卫星导航系统 BDS (BeiDou navigation satellite system)等物联网技术对生产信息、加工信息、运输信息以及销售信息按照一定的格式发送到数据中心进行“一物一码”标识,将搜集的数据自动上传区块链存证,利用区块链技术保证数据的隐私保护和不可篡改[119]。消费者或监管部门可通过追溯码查询商品流通环节数据信息,实现“一物一码”正品追溯。从中可以看出,物联网技术和区块链技术相辅相成,二者结合将会实现物理世界和数字世界的映射,实现农产品供应链中的数字孪生。

5.2.2 区块链 + 大数据

区块链技术具有加密共享、去中心化、信息防篡改等特性,对解决数据流通、价值共享、数据孤岛等方面提供了解决方案,而大数据技术具备海量数据存储和灵活高效的深度分析挖掘等功能,二者有机融合不仅保证了大数据分析结果的正确性和数据挖掘效果,还极大提升区块链数据的价值和使用空间。大数据管理聚合海量数据,将离散的数据需求聚合成数据长尾从而满足数据治理需求。运用大数据管理的虚拟性有利于追溯信息跨行业、跨生态的应用和管理,避免供应链各环节存在的断链情况,准确关联各环节的追溯信息,提供精准、完整的追溯数据。赵嘉承等[120]从大数据挖掘角度剖析区块链追溯过程中的信息真实性问题。CHEN 等[121]设计的农产品监管系统使用云计算技术进行追溯环节中物联网应用产生的大数据处理,并结合机器学习技术,建立模型预测对作物品种选择、生产和栽培管理以及上市时间等给出最佳的选择方案。

5.2.3 区块链 + 人工智能

区块链技术能够链接供应链各环节信息,促进跨行业、跨生态的数据流动、共享,让人工智能可以根据不同用途、需求获取更加全面的数据,真正变得“智能”。利用区块链 + 人工智能技术研发农产品可信追溯系统,把追溯技术从过去的纯数字空间防伪保护,升级为“物理空间 + 数字空间”的联合保护,同时使用人工智能技术结合机器学习边缘计算、自动化控制研发高速追溯数据采集系统,通过深度学习方法等自动识别农产品复杂供应链条中生产、加工、物流、销售等全环节人工干预的操作,实现行为数据上链存证保证数据的不可篡改将是二者结合的重要方向。

参 考 文 献

[1] AIK J, TURNER R M, KIRK M D, et al. Evaluating food safety management systems in singapore: a controlled interrupted time-series analysis of foodborne disease outbreak reports[J]. Food Control, 2020, 117: 107324.

[2] YUAN J J, LU Y L, CAO X H, et al. Regulating wildlife conservation and food safety to prevent human exposure to novel virus [J]. Ecosystem Health and Sustainability, 2020, 6(1): 1741325.

[3] HOU D Y, O'CONNER D, IGALAVITHANA A D, et al. Metal contamination and bioremediation of agricultural soils for food safety and sustainability[J]. Nature Reviews Earth & Environment, 2020, 1(7): 366 - 381.

[4] WANT R. A key to automating everything[J]. Scientific American, 2004, 290(1): 56 - 65.

[5] KING T S. Using QR codes on professional posters to increase engagement and understanding[J]. Nurse Educator, 2020, 45(4): 219.

[6] TAO M, LI X Q, YUAN H Q, et al. UAV-aided trustworthy data collection in federated-WSN-enabled IoT applications[J]. Information Sciences, 2020, 532: 155 - 169.

[7] 张京敏, 黄彦. 农产品供应链标准化体系构建及实现路径[J]. 北方园艺, 2020, 44(7): 166 - 170.
ZHANG Jingmin, HUANG Yan. Research on the construction of agricultural product supply chain standardization system[J]. Northern Horticulture, 2020, 44(7): 166 - 170. (in Chinese)

[8] 钱建平, 邢斌, 解菁, 等. 基于条码溯源电子秤的社区菜店交易管理与追溯系统[J/OL]. 农业机械学报, 2015, 46(5): 273 - 278, 292.
QIAN Jianping, XING Bin, XIE Jing, et al. Transaction management and traceability system of community vegetable shop based on barcode traceability scales[J/OL]. Transactions of the Chinese Society for Agricultural Machinery, 2015, 46(5): 273 - 278, 292. http://www.jcsam.org/jcsam/ch/reader/view_abstract.aspx? flag = 1&file_no = 20150539&journal_id = jcsam. DOI: 10.6041/j.issn.1000-1298.2015.05.039. (in Chinese)

[9] BEHZADI G, O'SULLIVAN M J, OLSEN T L. On metrics for supply chain resilience[J]. European Journal of Operational Research, 2020, 287(1): 145 - 158.

[10] 张长贵, 张岩峰, 李晓华, 等. 区块链新技术综述:图型区块链和分区型区块链[J]. 计算机科学, 2020, 47(10): 282 - 289.
ZHANG Changgui, ZHANG Yanfeng, LI Xiaohua, et al. Survey of new blockchain techniques: DAG based blockchain and Sharding based blockchain[J]. Computer Science, 2020, 47(10): 282 - 289. (in Chinese)

[11] 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 blockchain[J/OL]. Transactions of the Chinese Society for Agricultural Machinery, 2020, 51(8): 328 - 335. http://www.jcsam.org/jcsam/ch/reader/view_abstract.aspx? flag = 1&file_no = 20200836&journal_id = jcsam. DOI: 10.6041/j.issn.1000-1298.2020.08.036. (in Chinese)

[12] KORPELA K, HALLIKAS J, DAHLBERG T. Digital supply chain transformation toward blockchain integration[C]// International Conference on System Sciences, Hawaii, 2017: 1 - 10.

[13] KSHETRI N. Blockchain's roles in meeting key supply chain management objectives[J]. International Journal of Information Management, 2018, 39: 80 - 89.

[14] MEZQUITA Y, GONZALEZBRIONES A, CASADOVARA R, et al. Blockchain-based architecture: a mas proposal for efficient agri-food supply chains[C]// International Symposium on Ambient Intelligence, Hawaii, 2019: 89 - 96.

[15] KAMILARIS A, FONTS A, PRENAFETABOLDV F X. The rise of blockchain technology in agriculture and food supply chains [J]. Trends in Food Science and Technology, 2019, 91(1): 640 - 652.

[16] FRANCISCO K, SWANSON D. The supply chain has no clothes: technology adoption of blockchain for supply chain transparency[J]. Logistics, 2018, 2(1): 2.

[17] AZZI R, CHAMOUN R K, SOKHN M. The power of a blockchain-based supply chain[J]. Computers & Industrial Engineering, 2019, 135: 582 - 592.

[18] LU Q H, XU X W. Adaptable blockchain-based systems: a case study for product traceability[J]. IEEE Software, 2017, 34(6): 21 - 27.

[19] BUMBLAUSKAS D, MANN A, DUGAN B, et al. A blockchain use case in food distribution: do you know where your food has been? [J]. International Journal of Information Management, 2020, 52: 102008.

[20] ZHAO G Q, LIU S F, LOPEZ C, et al. Blockchain technology in agri-food value chain management: a synthesis of applications, challenges and future research directions[J]. Computers in Industry, 2019, 109: 83 - 99.

[21] KAMATH R. Food traceability on blockchain: Walmart's pork and mango pilots with IBM[J]. The Journal of the British Blockchain Association, 2018(1): 47 - 53.

[22] 杨信廷, 钱建平, 孙传恒, 等. 农产品及食品质量安全追溯系统关键技术研究进展[J/OL]. 农业机械学报, 2014, 45(11): 212 - 222.
YANG Xinting, QIAN Jianping, SUN Chuanheng, et al. Key technologies for establishment agricultural products and food quality safety traceability systems[J/OL]. Transactions of the Chinese Society for Agricultural Machinery, 2014, 45(11): 212 - 222. http://www.jcsam.org/jcsam/ch/reader/view_abstract.aspx? flag = 1&file_no = 20141133&journal_id = jcsam. DOI: 10.6041/j.issn.1000-1298.2014.11.033. (in Chinese)

[23] 国家市场监督管理总局、中国国家标准化管理委员会. 重要产品追溯追溯术语:GB/T 38155—2019[S]. 北京:中国标

准出版社, 2019.
[24] 赵春江, 郝玲, 杨信廷,等. 农产品视频履历追溯系统设计[J/OL]. 农业机械学报,2012,43(12): 118 - 122.
ZHAO Chunjiang, HAO Ling, YANG Xinting, et al. Design of video record for agricultural products traceability system[J/OL]. Transactions of the Chinese Society for Agricultural Machinery, 2012, 43(12): 118 - 122. http://www.jcsam.org/jcsam/ch/reader/view_abstract.aspx? flag = 1&file_no = 20121222&journal_id = jcsam. DOI: 10.6041/j.issn.1000-1298.2012.12.022. (in Chinese)
[25] 赵丽, 邢斌, 李文勇,等. 基于手机二维条码识别的农产品质量安全追溯系统[J/OL]. 农业机械学报,2012,43(7): 124 - 129.
ZHAO Li, XING Bin, LI Wenyong, et al. Agricultural products quality and safety traceability system based on two-dimension barcode recognition of mobile phones[J/OL]. Transactions of the Chinese Society for Agricultural Machinery, 2012, 43(7): 124 - 129. http://www.jcsam.org/jcsam/ch/reader/view_abstract.aspx? flag = 1&file_no = 20120723&journal_id = jcsam. DOI: 10.6041/j.issn.1000-1298.2012.07.023. (in Chinese)
[26] 杨信廷, 钱建平, 范蓓蕾,等. 农产品物流过程追溯中的智能配送系统[J]. 农业机械学报, 2011,42(5): 125 - 130.
YANG Xinting, QIAN Jianping, FAN Beilei, et al. Establishment of intelligent distribution system applying in logistics process traceability for agricultural product[J]. Transactions of the Chinese Society for Agricultural Machinery, 2011, 42(5): 125 - 130. (in Chinese)
[27] 孙传恒, 杨信廷, 李文勇,等. 基于监管的分布式水产品追溯系统设计与实现[J]. 农业工程学报,2012,28(8): 146 - 153.
SUN Chuanheng, YANG Xinting, LI Wenyong, et al. Design and realization of distributed traceability system of aquatic products based on supervision mode[J]. Transactions of the CSAE, 2012, 28(8): 146 - 153. (in Chinese)
[28] 杨信廷, 钱建平, 孙传恒,等. 蔬菜安全生产管理及质量追溯系统设计与实现[J]. 农业工程学报,2008,24(3): 162 - 166.
YANG Xinting, QIAN Jianping, SUN Chuanheng, et al. Design and application of safe production and quality traceability system for vegetable[J]. Transactions of the CSAE, 2008, 24(3): 162 - 166. (in Chinese)
[29] ZHAO T J, NAKANO A. Agricultural product authenticity and geographical origin traceability-use of nondestructive measurement[J]. JARQ-Japan Agricultural Research Quarterly, 2018, 52(2): 115 - 122.
[30] 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)
[31] 王媛,蔡友琼,徐捷. 国内外可追溯体系现状及我国水产品可追溯存在的问题[J]. 中国渔业质量与标准,2012,2(2): 75 - 78.
WANG Yuan, CAI Youjie, XU Jie. The current status of the traceability system at home and abroad and problems of traceability of aquatic products in China[J]. Chinese Fishery Quality and Standards, 2012, 2(2): 75 - 78. (in Chinese)
[32] KOMALAVALLI C, SAXENA D, LAROIYA C. Handbook of research on blockchain technology[M]. Academic Press, 2020: 349 - 371.
[33] 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)
[34] PEARSON S, MAY D, LEONTIDIS G, et al. Are distributed ledger technologies the panacea for food traceability? [J]. Global Food Security, 2019, 20: 145 - 149.
[35] FERNANDEZ E G, MORALESLUNA G, SAGOLS F. A zero-knowledge proof system with algebraic geometry techniques[J]. Applied Sciences, 2020, 10(2): 465.
[36] RIPEANU M. Peer-to-peer architecture case study: gnutella network [C] // International Conference on Peer-to-Peer Computing, Linkoping, 2001: 99 - 100.
[37] ATIGHEHCHI K. A precise non-asymptotic complexity analysis of parallel hash functions without tree topology constraints[J]. Journal of Parallel and Distributed Computing, 2020, 137: 246 - 251.
[38] TANG H M, SHI Y, DONG P W. Public blockchain evaluation using entropy and TOPSIS [J]. Expert Systems with Applications, 2019, 117: 204 - 210.
[39] PONGNUMKUL S, SIRIPANPORNCHANA C, THAJCHAYAPONG S. Performance analysis of private blockchain platforms in varying workloads[C]//26th International Conference on Computer Communication and Networks (ICCCN), Vancouver, BC, 2017: 1 - 6.
[40] LI Z T, KANG J W, YU R, et al. Consortium blockchain for secure energy trading in industrial internet of things[J]. IEEE Transactions on Industrial Informatics, 2018, 14(8): 3690 - 3700.
[41] GAI K K, WU Y L, ZHU L H, et al. Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks[J]. IEEE Internet of Things Journal, 2019, 6(5): 7992 - 8004.
[42] ZHOU T, LI X F, ZHA H. DLattice: a permission-less blockchain based on dpos-ba-dag consensus for data tokenization[J]. IEEE Access, 2019, 7: 39273 - 39287.
[43] YANG Z, YANG K, LEI L, et al. Blockchain-based decentralized trust management in vehicular networks[J]. IEEE Internet of Things Journal, 2019, 6(2): 1495 - 1505.
[44] 工业和信息化部信息中心. 2018 年中国区块链产业白皮书[R]. 2018: 60 - 64.
[45] 可信区块链推进计划溯源应用项目组. 区块链溯源应用白皮书(1.0)[R]. 2018.
[46] BETTIN-DIAZ R, ROJAS A E, MEJIA -MONCAYO C. Methodological approach to the definition of a blockchain system for

the food industry supply chain traceability[C]//Computational Science and Its Applications, Melbourne, VIC, 2018: 19 - 33.
[47] 腾讯研究院. 2019 腾讯区块链白皮书[R]. 2019.
[48] 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)
[49] SHIH D, LU K, SHIH Y, et al. A simulated organic vegetable production and marketing environment by using ethereum[J]. Electronics, 2019, 8(11): 1341.
[50] SALAH K, NIZAMUDDIN N, JAYARAMAN R, et al. Blockchain-based soybean traceability in agricultural supply chain[J]. IEEE Access, 2019, 7: 73295 - 73305.
[51] LIN Q J, WANG H Z, PEI X F, et al. Food safety traceability system based on blockchain and EPCIS[J]. IEEE Access, 2019, 7: 20698 - 20707.
[52] HONG W B, CAI Y F, YU Z R, et al. An agri-product traceability system based on IoT and blockchain technology[C]//1st IEEE International Conference on Hot Information-Centric Networking, 2018: 254 - 255.
[53] HAO Z H, MAO D H, ZHANG B, et al. A novel visual analysis method of food safety risk traceability based on blockchain[J]. International Journal of Environmental Research and Public Health, 2020, 17(7): 2300.
[54] HANG L, ULLAH I, KIM D H. A secure fish farm platform based on blockchain for agriculture data integrity[J]. Computers and Electronics in Agriculture, 2020, 170: 105251.
[55] ZHANG X, SUN P C, XU J P, et al. Blockchain-based safety management system for the grain supply chain[J]. IEEE Access, 2020, 8: 36398 - 36410.
[56] GORENFLO C, LEE S, GOLAB L, et al. FastFabric: scaling Hyperledger fabric to 20 000 transactions per second[C]//IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Seoul, 2019: 455 - 463.
[57] 陈纯. 联盟区块链关键技术与区块链的监管挑战[J]. 电力设备管理, 2019(11): 20 - 21, 28.
[58] 陆雯珺, 徐巧云, 李超. 可信环境下数据交易协同机制研究及应用[J]. 现代计算机, 2017(32): 45 - 51.
LU Wenjun, XU Qiaoyun, LI Chao. Research and applications of the coordination mechanism of data exchange in a trusted environment [J]. Modern Computer, 2017(32): 45 - 51. (in Chinese)
[59] 李鑫. Hyperledger Fabric 技术内幕:架构原理与实现原理[M]. 北京:机械工业出版社, 2019.
[60] CALDARELLI G, ROSSIGNOLI C, ZARDINI A. Overcoming the blockchain oracle problem in the traceability of non-fungible products[J]. Sustainability, 2020, 12(6): 2391.
[61] WANG S, LU H, SUN X K, et al. A novel blockchain oracle implementation scheme based on application specific knowledge engines[C]//IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI), Zhengzhou, 2019: 258 - 262.
[62] ADLER J, BERRYHILL R, VENERIS A, et al. Astraea: a decentralized blockchain oracle[C]//Green Computing and Communications, Halifax, 2018: 1145 - 1152.
[63] LO S K, XU X W, STAPLES M, et al. Reliability analysis for blockchain oracles[J]. Computers & Electrical Engineering, 2020, 83: 106582.
[64] DZIEMBOWSKI S, FAUST S, HOSTAKOVA K. General state channel networks[C]//ACM SIGSAC Conference on Computer and Communications Security, New York, 2018: 949 - 966.
[65] PODGORELEC B, HERICKO M, TURKANOVIC M. State channel as a service based on a distributed and decentralized web [J]. IEEE Access, 2020, 8: 64678 - 64691.
[66] MASHRU H, KABRA N, MOHAN K. A systematic framework for state channel protocols identification for blockchain-based IoT networks and applications[C]//IEEE International Conference on Communications Workshops, Dublin, 2020.
[67] 宋俊典, 戴炳荣, 蒋丽雯,等. 基于区块链的数据治理协同方法[J]. 计算机应用,2018,38(9): 2500 - 2506.
SONG Jundian, DAI Bingrong, JIANG Liwen, et al. Data governance collaborative method based on blockchain[J]. Journal of Computer Applications, 2018, 38(9): 2500 - 2506. (in Chinese)
[68] SHEN M, DUAN J X, ZHU L H, et al. Blockchain-based incentives for secure and collaborative data sharing in multiple clouds[J]. IEEE Journal on Selected Areas in Communications, 2020, 38(6): 1229 - 1241.
[69] CARRARA G R, BURLE L M, MEDEIROS D S V, et al. Consistency, availability, and partition tolerance in blockchain: a survey on the consensus mechanism over peer-to-peer networking[J]. Annales Des Télécommunications, 2020, 75: 163 - 174.
[70] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system [EB/OL]. https://bitcoin.org/bitcoin.pdf, 2008.
[71] QUANTUM M. Proof of stake [EB/OL]. https://bitcointalk.com, 2011.
[72] ZHENG Z B, XIE S A, DAI H N, et al. An overview of blockchain technology: architecture, consensus, and future trends[C]//IEEE 6th International Congress on Big Data, Honolulu, 2017.
[73] CASTR M, LISKOV B. Practical byzantine fault tolerance and proactive recovery[J]. ACM Transactions on Computer Systems, 2002, 20(4): 398 - 461.
[74] ONGARO D, OUSTERHOUT J. In search of an understandable consensus algorithm[C]//USENIX Annual Technical Conference, Philadelphia, 2014: 305 - 319.
[75] 张利, 童舟. 基于区块链技术的农产品溯源体系研究[J]. 江苏农业科学,2019,47(13): 245 - 249.
ZHANG Li, TONG Zhou. Study on traceability system of agricultural products based on blockchain technology[J]. Jiangsu Agricultural Sciences, 2019, 47(13): 245 - 249. (in Chinese)
[76] LENG K J, BI Y, JING L B, et al. Research on agricultural supply chain system with double chain architecture based on

blockchain technology[J]. Future Generation Computer Systems,2018,86: 641 - 649.
[77] 梁昊, 刘思辰, 张一诺,等. 农产品信息区块链技术架构设计及应用展望[J]. 智慧农业,2019, 1(1): 67 - 75.
LIANG Hao, LIU Sichen, ZHANG Yinuo,et al. Framework design and application prospect of agricultural product information blockchain[J]. Smart Agriculture,2019,1(1): 67 - 75. (in Chinese)
[78] 袁勇, 倪晓春, 曾帅, 等. 区块链共识算法的发展现状与展望[J]. 自动化学报,2018,44(11): 2011 - 2022.
YUAN Yong, NI Xiaochun, ZENG Shuai,et al. Blockchain consensus algorithms: the state of the art and future trends[J]. Acta Automatica Sinica,2018,44(11): 2011 - 2022. (in Chinese)
[79] 任守纲, 何自明, 周正己,等. 基于 CSBFT 区块链的农作物全产业链信息溯源平台设计[J]. 农业工程学报,2020,36(3): 279 - 286.
REN Shougang, HE Ziming, ZHOU Zhengji,et al. Design and implementation of information tracing platform for crop whole industry chain based on CSBFT-blockchain[J]. Transactions of the CSAE,2020,36(3): 279 - 286. (in Chinese)
[80] 王志铧, 柳平增, 宋成宝,等. 基于区块链的农产品柔性可信溯源系统研究[J]. 计算机工程,2020,46(12):313 - 320.
WANG Zhihua, LIU Pingzeng, SONG Chengbao,et al. Research and development of flexible and reliable traceability system for agricultural products base on blockchain[J]. Computer Engineering, 2020, 46(12):313 - 320. (in Chinese)
[81] YAGA D, MELL P, ROBY N,et al. Blockchain technology overview[J]. arXiv preprint arXiv, 2019,1906: 11078.
[82] CHAPRON G. The environment needs cryptogovernance[J]. Nature,2017,545: 403 - 405.
[83] 李文勇, 孙传恒, 刘学馨,等. 水产品追溯码加密算法设计与应用[J/OL]. 农业机械学报,2012, 43(4): 106 - 112.
LI Wenyong, SUN Chuanheng, LIU Xuexin,et al. Design and implementation of encryption algorithm for aquatic products traceability code[J/OL]. Transactions of the Chinese Society for Agricultural Machinery,2012,43(4): 106 - 112. http://www.jcsam.org/jcsam/ch/reader/view_abstract.aspx? flag = 1&file_no = 20120421&journal_id = jcsam. DOI:10.6041/j.issn.1000-1298.2012.04.021. (in Chinese)
[84] 马腾, 孙传恒, 李文勇,等. 基于 NB - IoT 的农产品原产地可信溯源系统设计与实现[J]. 中国农业科技导报,2019,21(12): 58 - 67.
MA Teng, SUN Chuanheng, LI Wenyong,et al. Design and implementation of trusted traceability system for agricultural products origin based on NB - IoT[J]. Journal of Agricultural Science and Technology, 2019,21(12): 58 - 67. (in Chinese)
[85] 张旭凤, 宛如星, 郑忠义. 基于区块链技术的农产品物流信息系统模式[J]. 江苏农业科学, 2019, 47(15): 263 - 268.
ZHANG Xufeng, WAN Ruxing, ZHENG Zhongyi. Agricultural products logistics information system model based on block chain technology[J]. Jiangsu Agricultural Sciences,2019,47(15): 263 - 268. (in Chinese)
[86] 王乃洲, 金连文, 高兵. 基于区块链技术的身份认证与存储方法研究[J]. 现代信息科技, 2020,4(8): 164 - 167.
WANG Naizhou, JIN Lianwen, GAO Bing. Research on identity authentication and storage method based on blockchain technology[J]. Modern Information Technology, 2020,4(8): 164 - 167. (in Chinese)
[87] 徐蜜雪, 苑超, 王永娟,等. 拟态区块链——区块链安全解决方案[J]. 软件学报,2019,30(6): 1681 - 1691.
XU Mixue, YUAN Chao, WANG Yongjuan,et al. Mimic blockchain—solution to the security of blockchain[J]. Journal of Software,2019,30(6): 1681 - 1691. (in Chinese)
[88] 李宣, 柳毅. 基于双区块链及物联网技术的防伪溯源系统[J]. 计算机应用研究,2020,37(11):1 - 6.
LI Xuan, LIU Yi. Traceability system based on double blockchain and internet of things technology[J]. Application Research of Computers, 2020,37(11): 1 - 6. (in Chinese)
[89] 李佳潞. 基于区块链的粮食供应链溯源方案的研究[D]. 北京: 北京邮电大学, 2019.
LI Jialu. Research on traceability scheme of grain supply chain based on blockchain[D]. Beijing: Beijing University of Posts and Telecommunications,2019. (in Chinese)
[90] 黄建华, 江亚慧, 李忠诚. 利用区块链构建公平的安全多方计算[J]. 计算机应用研究,2020, 37(1): 225 - 230,244.
HUANG Jianhua, JIANG Yahui, LI Zhongcheng. Constructing fair secure multi-party computation based on blockchain[J]. Application Research of Computers,2020,37(1): 225 - 230,244. (in Chinese)
[91] 蚂蚁集团. 蚂蚁链溯源营销服务解决方案[R/OL]. available: https://survey.aliyun.com/apps/zhiliao/DQyghh9AO? source = , 2020.
[92] 京东集团. 京东区块链技术实践白皮书(2019)[R]. 2019.
[93] 郭明明. 运用区块链技术提升农业发展水平——以黑龙江北大荒区块链数字农业股份有限公司为例[J]. 农场经济管理,2018(12): 17 - 19.
GUO Mingming. Using blockchain technology to improve the level of agricultural development—taking Heilongjiang Beidahuang blockchain digital agriculture compony as an example[J]. Farm Economic Management, 2018(12): 17 - 19. (in Chinese)
[94] ESMAEILIAN B, SARKIS J, LEWIS K,et al. Blockchain for the future of sustainable supply chain management in Industry 4.0[J]. Resources Conservation and Recycling,2020,163: 105064.
[95] ZHAO Z Y, MIN K J. Blockchain traceability valuation for perishable agricultural products under demand uncertainty[J]. International Journal of Operations Research and Information Systems (IJORIS),2020,11(4): 1 - 32.
[96] 吕芙蓉, 陈莎. 基于区块链技术构建我国农产品质量安全追溯体系的研究[J]. 农村金融研究, 2016(12): 22 - 26.
LÜ Furong, CHEN Sha. Research on constructing my country's agricultural product quality and safety traceability system based on blockchain technology[J]. Rural Finance Research,2016(12): 22 - 26. (in Chinese)
[97] 余斌, 李晓风, 赵赫. 基于区块链存储扩展的结构化数据管理方法[J]. 北京理工大学学报, 2019,39(11): 1160 - 1166.
YU Bin, LI Xiaofeng, ZHAO He. Structured data management method based on scalable blockchain storage[J]. Transactions of Beijing Institute of Technology,2019,39(11):1160 - 1166. (in Chinese)

[98] KAN L, WEI Y, MUHAMMAD A H, et al. A multiple blockchains architecture on inter-blockchain communication[C]// IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), Lisbon, 2018: 139-145.
[99] CHEN X, ZHANG K J, LIANG X B, et al. HyperBSA: a high-performance consortium blockchain storage architecture for massive data[J]. IEEE Access, 2020(8): 178402-178413.
[100] NORTA A, WENNA C, UDOKWU C. Designing a collaborative construction-project platform on blockchain technology for transparency, traceability and information symmetry[R]. ResearGate, 2020.
[101] KOHLER S, PIZZOL M. Technology assessment of blockchain-based technologies in the food supply chain[J]. Journal of Cleaner Production, 2020, 269: 122193.
[102] LIAO S Y, WU J, LI J H, et al. Proof-of-balance: game-theoretic consensus for controller load balancing of SDN[C]// IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Toronto, 2020: 231-236.
[103] 刘家稷, 杨挺, 汪文勇. 使用双区块链的防伪溯源系统[J]. 信息安全学报, 2018, 3(3): 17-29.
LIU Jiaji, YANG Ting, WANG Wenyong. Traceability system using public and private blockchain[J]. Journal of Cyber Security, 2018, 3(3): 17-29. (in Chinese)
[104] DING Q Y, GAO S, ZHU J M, et al. Permissioned blockchain-based double-layer framework for product traceability system [J]. IEEE Access, 2020, 8: 6209-6225.
[105] HINTEREGGER A, HASLHOFER B. An empirical analysis of monero cross-chain traceability[C]// 23rd International Conference on Financial Cryptography and Data Security, Grenada, 2019: 150-157.
[106] JIANG Y M, WANG C X, HUANG Y, et al. A cross-chain solution to integration of IoT tangle for data access management [C]// IEEE Confs on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, Congress on Cybermatics, Halifax, NS, 2018: 1035-1041.
[107] JIANG Y M, WANG C X, WANG Y, et al. A cross-chain solution to integrating multiple blockchains for IoT data management[J]. Sensors, 2019, 19(9): 2042.
[108] YANG S L, WANG H M, LI W, et al. CVEM: A cross-chain value exchange mechanism[C]// 3th International Conference on Cloud Computing and Internet of Things, Dalian, 2018: 80-85.
[109] 赵子军. 数字赋能标准引领——2019 新一代信息技术产业标准化论坛成功举办[J]. 中国标准化, 2019(17): 38-40.
[110] 钱建平, 吴文斌, 杨鹏. 新一代信息技术对农产品追溯系统智能化影响的综述[J]. 农业工程学报, 2020, 36(5): 182-191.
QIAN Jianping, WU Wenbin, YANG Peng. Review on agricultural products smart traceability system affected by new generation information technology[J]. Transactions of the CSAE, 2020, 36(5): 182-191. (in Chinese)
[111] ALI M S, VECCHIO M, PINCHEIRA M, et al. Applications of blockchains in the internet of things: a comprehensive survey [J]. IEEE Communications Surveys and Tutorials, 2019, 21(2): 1676-1717.
[112] FERNANDEZ-CARAMES T M, FRAGA-LAMAS P. A review on the use of blockchain for the internet of things[J]. IEEE Access, 2018, 6: 32979-33001.
[113] TIAN F. An agri-food supply chain traceability system for China based on RFID blockchain technology[C]// 13th International Conference on Service Systems and Service Management, 2016.
[114] BORDEL B, LEBIGOT P, ALCARRIA R, et al. Digital food product traceability: using blockchain in the international commerce[C]// International Conference on Digital Science, 2019: 224-231.
[115] 何正源, 段田田, 张颖, 等. 物联网中区块链技术的应用与挑战[J]. 应用科学学报, 2020, 38(1): 22-33.
HE Zhengyuan, DUAN Tiantian, ZHANG Ying, et al. Blockchain in internet of things: application and challenges[J]. Journal of Applied Sciences, 2020, 38(1): 22-33. (in Chinese)
[116] 刘耀宗, 刘云恒. 基于区块链的 RFID 大数据安全溯源模型[J]. 计算机科学, 2018, 45(11A): 367-368, 381.
LIU Yaozong, LIU Yunheng. Security provenance model for RFID big data based on blockchain[J]. Computer Science, 2018, 45(11A): 367-368, 381. (in Chinese)
[117] LIN J, ZHANG A T, SHEN Z Q, et al. Blockchain and IoT based food traceability for smart agriculture[C]// 3rd International Conference on Crowd Science and Engineering, Kunming, 2018.
[118] CARO M P, ALI M S, VECCHIO M, et al. Blockchain-based traceability in agri-food supply chain management: a practical implementation[C]// IoT Vertical and Topical Summit on Agriculture-Tuscany (IOT Tuscany), Tuscany, 2018: 1-4.
[119] FENG L B, ZHANG H, LOU L Q, et al. A blockchain-based collocation storage architecture for data security process platform of WSN[C]// IEEE 22nd International Conference on Computer Supported Cooperative Work in Design (CSCWD), Nanjing, 2018: 75-80.
[120] 赵嘉承, 郑新立, 陈浩, 等. 基于大数据挖掘的进口食用农产品质量安全数据开放共享研究[J]. 信息通信, 2020(4): 13-15.
ZHAO Jiacheng, ZHENG Xinli, CHEN Hao, et al. Research on open sharing of imported edible agricultural products quality and safety data based on big data mining[J]. Information & Communications, 2020(4): 13-15. (in Chinese)
[121] CHEN J B, CAO X L, FU H C, et al. Agricultural product monitoring system supported by cloud computing[J]. Cluster Computing, 2019, 22: S8929-S8938.