

doi: 10.19920/j.cnki.jmsc.2024.05.001

基于区块链的农产品供应链溯源研究综述^①

胡祥培¹, 都 牧^{1*}, 孔祥维², 朱 姍¹, 张源凯³

(1. 大连理工大学经济管理学院, 大连 116024; 2. 浙江大学管理学院, 杭州 310058;
3. 北京航空航天大学经济管理学院, 北京 100191)

摘要: 中国的农产品供应链是一个多利益主体共同参与、多阶段多链路、动态可扩展网链的人机复合系统, 使得基于区块链的农产品供应链溯源系统面临着链上信息泄露和溯源信息造假的管理实践挑战。本研究结合我国农产品供应链特点, 从建设基于区块链的农产品供应链溯源系统的实际需求以及应用实践出发, 对区块链技术及应用、区块链中的隐私保护与农产品信息安全、信任传递与融合方法这三个方面对国内外相关研究进行综述, 并据此提出我国建设这类溯源系统的两个核心难题——“如何建”和“如何查”。针对这两个难题, 从管理科学视角各提出四类关键科学问题, 展望未来研究的发展趋势, 并从应用实践层面提出基于区块链的农产品供应链溯源系统的发展建议。

关键词: 农产品供应链; 区块链; 质量追溯; 隐私保护与信息安全; 信任传递与融合

中图分类号: C931.2 **文献标识码:** A **文章编号:** 1007-9807(2024)05-0001-12

0 引 言

农业乃至农产品质量安全, 时刻影响着亿万百姓的生活, 关系到国民经济发展及社会安定, 是党和国家长期关注的重大问题。习近平总书记指出, 实施乡村振兴战略, 必须深化农业供给侧结构性改革, 走质量兴农之路。2019年2月11日出台的《国家质量兴农战略规划(2018年—2022年)》明确提出, 要以质量兴农为目标, 完善标准、严格监管、健全体系^[1]。强化农产品质量溯源是实施质量兴农战略的重要手段, 构建可信的农产品供应链溯源体系势在必行。

近年来国内外学术界和产业界在物联网的基础上, 利用区块链的去中心化(分布式)、不可篡改性、透明性等特性, 建立起农产品质量溯源防伪系统, 为构建高效、透明、安全、可靠的“一键式”农产品供应链溯源体系创造了十分优越的技术条

件和实施手段, 大幅提高了农产品造假“作恶”门槛。特别是2019年12月以来, 党中央、国务院和农业农村部多次召开会议并发布文件, 指示要大力发展推进基于“物联网+区块链”的农产品的质量安全溯源, 以解决“三农”问题。2020年2月5日, 中央一号文件又聚焦“三农领域”, 提出“加快区块链等现代信息技术在农业领域的应用”。可见, 党和国家已经将区块链技术作为发展智慧农业、促进质量兴农、解决“三农”问题的重要手段, 引起了社会各界的广泛关注。

随着我国质量兴农战略的推进, 近几年全国各大农业产区以及众多知名企业(京东、阿里巴巴、腾讯、海尔等)运用区块链和物联网等现代信息技术纷纷抢滩现代农业技术高地, 先后涌现出一大批基于区块链和物联网的智慧农场(如京东农场、京东牧场——“跑步鸡”、智链 ChainNova “区块链大农场”、海尔食联网平台等)及相应的

^① 收稿日期: 2020-11-02; 修订日期: 2023-01-13。

基金项目: 国家自然科学基金资助重点国际(地区)合作研究项目(72010107002); 辽宁省博士科研启动基金资助项目(2020-BS-064)。

通讯作者: 都 牧(1988—), 女, 辽宁庄河人, 博士, 副教授。Email: dumu@dlut.edu.cn

质量溯源系统,开启了我国质量兴农的智慧农业发展之路.然而,作者近年来结合国家自然科学基金重点项目和国家自然科学基金创新研究群体科学基金项目等项目的研究以及与京东集团合作开展的“京东农场”示范工程建设实践深深体会到:智慧农场虽然可以大大提高消费者的信任度,从而形成“优质优价+价值共创”的新模式,且已取得明显成效,但是基于区块链的农产品溯源新平台面对新机遇的同时,又伴随着许多新挑战.例如,信息共享过程中敏感数据泄露的高风险、上链数据的源头造假、溯源求证追责困难、建设信任机制任重道远等.所以,虽然区块链可以解决农产品供应链中的信息孤岛难题,但是仅仅依靠技术还不能从根本上实现农产品供应链的可信溯源,基于区块链技术的质量兴农之路依然困难重重.

具体而言,基于区块链技术的质量兴农之路的难点归纳为:链上数据安全与隐私保护(信息安全)、溯源信息可信性(信息造假)等.其原因在于,农产品供应链溯源系统是一个多种信息技术高度集成、多利益主体共同参与、从“农田到餐桌”的多阶段、多链路、动态可扩展网链的人机复合系统^[5],它包括种植、采摘、包装、运输、仓储、销售等多个环节,且人工操作较多.在链上数据安全与隐私保护方面,农产品供应链中参与主体众多,并且参与方式弹性多变,区块链分布式、透明性的特征很容易导致参与主体敏感数据的泄露.在溯源信息可信性方面,由于区块链技术只是保证了区块链网络中数据的不可篡改,但无法保证在数据上链环节的真实有效性,一旦数据源头造假,链上数据即使不可篡改也毫无意义.所以,在建设基于区块链的农产品供应链溯源系统时,还需要重点关注信息安全和隐私保护方法以降低供应链参与方的链上信息安全风险,以及(信息的)信任传递与融合方法来识别上链信息造假、实现溯源防伪和求证问责.

本研究面向基于区块链的农产品供应链溯源实施过程中的实际难题,对国内外相关研究进行综述.首先,综述区块链技术及应用研究进展,其中包括了基于区块链的农产品供应链溯源相关研究现状.其次,针对实践中基于区块链的农产品供应链溯源面临的信息安全和信息造假两大难题,分别对区块链中的隐私保护与信息安全管理、信

任传递与融合理论与方法这两个领域的研究进展进行综述.最后,从管理科学的视角提出了基于区块链的农产品供应链溯源管理中的关键难题,并展望了基于区块链的农产品供应链溯源的未来研究趋势.

1 基于区块链的农产品供应链溯源的相关研究现状

1.1 区块链技术及应用的相关研究进展

近年来区块链市场呈现出爆发式增长趋势,区块链研究也受到了工业界以及学术界广泛关注^[2-4,6].目前,研究者对于区块链的研究可以分为两个方面:区块链的核心技术研究和区块链在各个行业中的应用研究.

关于区块链的核心技术研究主要集中在数据结构、网络结构、加密算法、共识机制/协议等方面,其目的主要是为了解决数据存储问题、信任问题以及隐私安全等问题.在数据结构方面,为了提高区块链系统的空间利用率和安全性、减少系统交易延迟,研究的热点主要集中在区块容量设计、区块存储设计、大规模多源数据存储设计等问题^[2].在网络结构方面,针对区块链存在可拓展性差、容量有限等问题,已经有学者设计了不同的网络结构(无结构对等网络、结构化对等网络和混合式对等网络)及相应的节点准入机制与通信传播机制^[2,6].在加密算法方面,为了实现数据防篡改、匿名性和隐私性,已有研究提出了多种加密算法,主要分为哈希函数(如 Ethash, Scrypt 等)、数字签名(如 ECDSA 等)、其他特殊加密算法(如 zero-knowledge proofs 等)三大类^[7].在共识机制/协议方面,研究的关键问题是如何在不可信的环境下实现账本数据的全网统一,已有研究主要提出了四类共识协议:基于激励奖惩机制的 PoX 类协议(如基于工作量证明的协议 Proof-of-Work),解决拜占庭容错问题的 BFT 类共识协议,基于崩溃容错的 CFT 类基础共识协议和混合型协议^[8-11].

此外,在区块链技术的研究中一个需要关注的领域是关于上链数据的真实性及完整性验证的研究.当前,不少学者对不同类型和来源的数据,

如,图像数据、视频数据、物联网数据、云存储数据等,进行了研究。代表性研究包括,Hirano等^[12]针对医疗临床试验数据造假和人工输入错误等问题,提出一种基于区块链的数据管理系统,保证临床数据的可信性和安全性。Khan等^[13]针对智慧城市中视频监控系统伪造视频数据的问题,提出一种基于区块链的视频数据检测-认证系统。Chimire等^[14]同样针对视频数据的伪造问题,提出一种新型基于区块链的视频数据完整性验证的方法。Li等^[15]利用区块链与物联网相结合的方式,提出一种针对IOT图像数据的传输与存储方案,可以解决物联网数据传输中数据盗窃和伪造等问题。Wei等^[16]针对云存储数据的完整性及安全性等问题,提出一种区块链分布式agent模型,保证数据的信任验证、数据监测及可靠性存储。在上述研究中,信任传递与融合是实现上链数据的真实性及完整性验证的重要手段,将在1.3节中综述这方面的研究进展。

将可追溯、不可篡改、公开透明、分布式可信等区块链特性与具体领域业务需求相结合,在不同的领域已取得明显成效。例如,在金融^[17,18]、制造业^[19,20]、能源^[21,22]、建筑^[23]、医疗^[15-18]、奢侈品^[24]等,区块链技术均有具有代表性的典型应用。而在供应链及食品安全管理领域,区块链技术通常被用于实现信息共享以及产品溯源^[25-27]。例如,在供应链管理领域,Di等^[28]研究了通过基于区块链的信息共享,实现供应链的可持续发展,Choi等^[29]研究了通过在航空供应链中进行信息共享降低供应链风险,Rahmanzadeh等^[30]研究了基于区块链和信息共享机制用于降低供应链中的不确定性,缓解供应链中的牛鞭效应,Wang等^[31]提出了供应链中基于区块链的数据共享模式和定价方法。此外,还有许多前瞻性研究探讨了将区块链应用于物流追溯系统,并结合物联网技术,实现对货物的识别、监控、追踪和溯源^[32-34]。在食品安全管理领域,基于区块链的食品追溯体系可以为相关监管部门和消费者提供从原材料到生产、加工、运输、销售再到消费者的全链条信息,为解决食品安全问题提供了一种行之有效的手段^[35-37]。此外,在进口产品溯源领域,区块链技术也有着相似的应用^[38]。

在农产品供应链溯源领域,已经有学者指出

区块链在其中能够发挥的革命性作用^[39,40]。传统的农产品供应链溯源系统和单纯依靠物联网技术的农产品溯源系统的相关研究可以分别参考Aung等^[41]和Ping等^[42]的综述文章,本研究将不作具体综述。而基于区块链的农产品溯源,面向不同类型农产品供应链的溯源需求,学者们也进行了针对性的研究。最早受到关注的此类研究就是沃尔玛联合IBM共同构建的中国猪肉区块链溯源系统和美洲芒果区块链溯源系统^[37]。Salah等^[36]利用区块链技术构建了针对大豆的农产品溯源系统,重点利用智能合约来管理和控制供应链中的所有交易。另外,针对粮食安全问题,Zhang等^[43]构建了一个基于区块链的粮食供应链安全管理系统,解决了粮食供应链中存在的信息孤岛、信息编码、商业隐私和数据存储的问题,同时指出信息安全管理、区块链存储的限制以及数据的可靠性保证是此类区块链系统需要重点关注的问题。此外,Feng^[44]针对中国农产品供应链安全中的供需匹配问题,提出了一种基于RFID和区块链的溯源系统。Hang等^[45]关注到了渔业数据被人工篡改的问题,提出一种将区块链与原始渔业养殖系统集成的实用方法,通过在区块链中存储数据实现链上数据防篡改,但是这一方法仍然无法保障上链过程中的数据可信性。特别是,Lin等^[46]指出食品供应链溯源中存在数据爆发、信任转移和敏感数据泄露这三个难题,现有区块链的溯源系统仍然需要进行改进甚至重构。而结合我国农产品供应链特点,这三大难题在建设区块链溯源系统过程中尤为凸显,这也与作者团队的实践经验相吻合。

综上所述,作为一种新兴技术,已有研究在区块链技术方面(数据结构,网络结构,加密算法,共识机制/协议等)已经取得了重大进展,对上链数据真实性和完整性验证技术也有所突破,并且区块链在各行各业都具有巨大的应用潜力。但将区块链技术应用到具体的供应链管理中,特别是农产品供应链溯源中,虽然已经取得了一些初步成效,仍存在着许多管理问题亟待解决。结合我国当前农产品供应链的实际,具体包括基于区块链的农产品溯源信息低冗余存储、基于区块链的农产品溯源信任链构建以及基于区块链的农产品溯源系统的信息安全这三个关键难题。这些挑战性难

题的解决需要结合区块链的分布式存储、匿名性、开放透明等技术特点以及农产品溯源领域中存在的多主体参与、海量数据存储、数据实时传输、数据防篡改等特点和实际需求,从而实现基于区块链的安全、可信农产品供应链溯源。

1.2 区块链中的隐私保护与信息安全管理的相关研究进展

区块链技术本身的特性(去中心化、匿名性、数据不可篡改)使其为解决分布式环境下实体间信任问题提供了有效的技术方案。然而,上述特性同时也使得区块链中包括账户、交易、电子合约等用户信息在整个网络中趋于透明化,亟需增加隐私保护机制。因此区块链中的隐私保护和信息安全管理也逐渐成为研究热点^[47,48]。

区块链的隐私和信息安全的威胁包括网络层、交易层和应用层三类,其中网络层的威胁主要是来自于恶意节点的接入和监听,交易层的威胁包括交易隐私威胁^[49]和身份隐私威胁^[6],应用层威胁主要是用户行为和区块链服务商导致的隐私泄露。针对上述不同的威胁种类,学者们提出了相应的技术方案。

区块链网络层隐私保护和信息安全管理的研究重点是提升攻击者搜集网络层中数据的难度^[50],主要技术包括三类:接入节点授权限制(区块链节点接入模式,例如超级账本)、检测恶意节点并屏蔽技术(节点通信机制)、以及网络层数据混淆(数据传输的协议机制,例如洋葱路由技术)。区块链交易层隐私保护和信息安全管理的研究重点是在保持区块链中的基本共识机制和数据存储不变的同时,对数据本身信息和潜在信息加以隐匿保护,防止攻击者通过分析区块数据提取用户画像,主要的技术包括三类:混币机制技术、数据加密技术以及基于限制发布的技术。混币机制技术是通过进行交易过程进行混淆来提升交易的安全性,可以分为中心节点混币方法^[51-53]和去中心化的混币方法^[54,55];数据加密技术是对区块链中需要进行隐私保护的内容(如交易内容、交易双方地址等)进行加密,主要包括采用门罗币的加密方案、数字签名^[56]、Ring CT2.0、Zcash的加密方案^[57];基于限制发布的技术是直接涉及隐私的数据信息从公开数据库中移除,包括联盟链和私有链技术^[58]、闪电网络技术^[59]。区块链应用层的隐私保

护和信息安全,是指对区块链数据被外部应用使用过程存在泄露交易隐私和身份隐私的保护,着重于使用者本身安全意识及安全防护水平的提升,例如在用户和服务商之间使用合理的公私钥保存机制、构建无漏洞的区块链服务等^[60]。现阶段的研究主要集中在向使用者提供具有隐私保护能力的区块链程序,以及如何提升使用者主观上的隐私保护意识。

综上所述,国内外学者对于区块链的隐私保护和信息安全管理的研究已经取得了丰富的成果和解决方案。但将这些隐私保护和信息安全管理机制应用到具体的供应链管理中,仍然存在公有链网络中恶意节点难以检测、传统的混币机制隐私保护性能不足等问题。同时,构建基于区块链的农产品供应链溯源系统时,需要将已有的隐私保护和信息安全机制与农产品供应链特点相结合。农产品供应链的溯源系统的隐私威胁主要来自交易层,而供应链中参与主体众多,且溯源过程需要对节点和链上数据进行监管,联盟链是合适的区块链架构。因此,如何设计监管友好型的联盟链基础架构,在保护隐私的前提下实现对多个参与主体的有效监管,是需要研究的主要问题。

1.3 信任传递与融合方法相关研究进展

信任传递和融合的概念起源于计算机网络安全领域,利用网络中已知可信任节点的相关或相邻节点的交互历史来推理判断未知节点的信任度,主要用于解决分布式网络中的可信性判断问题^[61]。其中,信任传递是指信息流在主体间依据某个路径从推荐者向接收者传递的过程,信任融合是指将来自于相同或不同信息源的多条信息链传递过来的同质或异质信息进行汇总融合的过程。

农产品质量溯源系统是多利益主体共同参与、从“农田到餐桌”多阶段、多链路、动态可扩展网链的人机复合系统,涉及环节和人工操作众多,数据来源多种多样。所以在数据上链和质量安全事故追溯过程中,需要对分布式系统中信息节点的可信性做出判断,通过数据融合和交叉验证,查找出造假数据和导致质量问题的环节。为了实现上述过程,需要利用信任传递模型和信任融合方法对上链数据以及链上数据(信息)进行可信判断。以下针对信任传递建模方法和信任融合方法

展开综述。

有关信任传递建模方法的研究,国内外学者主要从数学模型和网络模型两个角度进行了探索。基于数学模型的信任传递建模方法包括基于概率论的传递模型和基于模糊数学的传递模型。基于概率论的信任传递数学模型将主体间的信任度以概率形式表示,依托于概率论运算法则,有较为深厚的理论基础且计算方式简单易操作^[62]。而基于模糊理论信任传递数学模型,考虑了信任链传递过程中人的主观感受特性,与概率模型相比对主体信任感知的抽象更为丰富^[63]。基于网络模型的信任传递建模方法,利用复杂网络和图论的知识从网络演化层面分析信任传递机制,探索信任传递路径的求解方法^[64]。在信任传递机制方面,学者们大都采用实证研究方法分析信任网络结构特性^[65]。在信任传递路径求解方法方面,学者们通常以大规模、高复杂度的社交网络为研究契机,以减小计算复杂性、缩短计算时间为研究目标,寻找网络中信任传递的最佳路径。Richters等^[66]在信任传递过程中为了降低计算的时间和复杂性,用反向搜索方法寻找信任度最高的最短路径。Kim等^[67]考虑在线社交网络中信任传播时的信息过载问题,设计基于强化学习的信任度评估策略,比较并评估可用信任路径以寻找信任度最大化的最佳策略。

有关信任融合方法的研究,主要集中在多源异质信息的处理问题上,其中以D-S证据融合理论发展较为完善和成熟。D-S证据理论的原型于1967年由Dempster提出,其核心就是综合计算并融合多条信任链上的证据信息^[68]。Shafer在这一工作的基础上,将合成规则推广到更一般的情境,形成了Dempster-Shafer(D-S)证据融合理论^[69]。此后,许多学者从理论方法和应用领域方面不断扩展D-S证据融合研究领域的边界,包括:多属性决策方法^[70]、不确定多属性决策的证据推理方法^[71]、证据推理概率建模和规则的扩展方法^[72]、证据理论在风险评估^[73]、专家系统^[74]、运筹优化^[75]、数据处理^[76]等领域的应用研究。此外,也有学者从模糊理论、主观逻辑等角度进行信任融合方法的研究^[77]。

综上所述,信任问题起源于计算机网络安全领域,并逐渐拓展到信息系统、电子商务等研究领

域,在信任传递建模方法、信任融合方法等方面已经取得了较为丰硕的成果。但是,中国的农产品供应链富有中国特色(亿万“包产到户”式的分散式农户及其诱发的系列问题),如我国农产品供应链囊括的主体众多且能力各异(如大的电商平台和小农个体户)、农产品种类繁多且不同品种影响因素不同、从“农场到餐桌”涉及环节多等特点,使得农产品供应链上信息阶段的信任传递困难、信息体量大且源头不同导致多源信任融合困难,传统的信任传递与融合方法难以适用和求解我国农产品供应链的信任传递问题。因此,针对质量事故频发的农产品销售领域,结合我国农产品供应链的独特特点,基于区块链技术的分布式数据存储结构和物联网技术下的多源异构大数据,如何研究信任传递过程、构建信任传递模型、设计信任融合规则、计算综合信任度等是解决我国农产品质量追溯中溯源信息可信性这一问题的关键点。

1.4 研究现状小结

综上所述,国内外学术界和产业界在区块链技术及其应用(特别是农产品供应链溯源)已经开展了一系列研究,同时在隐私保护与信息安全管理、信任传递与融合方法等方面开展了众多前沿性研究,研究成果十分丰富,可以为后续的相关研究提供理论方法支撑与应用研究基础。但是,由于农产品质量溯源系统是多种信息技术高度集成、多利益主体共同参与、从“农田到餐桌”多阶段、多链路、动态可扩展网链的人机复合系统,具有高度的复杂性和挑战性,中国的农业、农村、农民又有中国特色,基于区块链的农产品溯源系统仍有如下关键难题至今未能根本解决,主要体现在:

1) “如何建?”——如何以较低的投入建立安全可信的基于区块链的农产品供应链溯源系统?

区块链的去中心化及分布式记账模式虽然从技术上保证了不可篡改性和透明性,但要求农产品供应链中“最先一公里”的每一个农户(特别是中国式包产到户的农户)和“最后一公里”中数量巨大的亿万消费者都独立记账并存储相关信息是不现实的。与此对应的棘手问题是在分布式架构体系下如何构建适应于中国分散式个体农户和大规模消费者的区块链溯源架构?此外还有如何建

立基于区块链的农产品溯源系统多方参与者的隐私保护机制和信息安全保障体系?这是学术界和产业界致力攻克和亟待解决的重点难题之一。

2) “如何查?”——如何实现该溯源系统快速高效的溯源查询、置信求证、问责治理?

区块链技术目前仅能保证上链数据不被篡改,但无法保证上链数据的真实性,而上链的生产和配送数据造假会无法确保对农残超标和违法保鲜化学物质等监测跟踪的有效性,进而无法对农产品保真、保质和保量,质量事故还是频发且难以追责。此外,食品质量安全问题关系到人民的生命健康,一旦发生会导致严重后果,因而不仅需要进行“事后”溯源,还需要在“事中”进行选案分析、识别风险。因此,如何对农产品质量安全风险或质量事故的感知、识别、预警、置信求证和问责治理,是需要研究的难题。现有的利用物联网自动采集技术、以及使用证据理论中的信任传递融合方法结合物流系统等多源信息进行交叉验证可以有效减少人为操纵、降低上链源数据假冒的可能性。但是,农产品供应链系统即使采用了区块链这一高新智能防伪技术,由于从“农田到餐桌”的种植、采摘、包装、运输、仓储、销售等环节人工作业较多,数据量大且数据源多种多样,传统的证据理论与方法难以解决此类置信求证问题,消费者查询到的溯源信息依然存在诸多可造假的漏洞,难以确认质量事故的证据和进行问责治理,信任机制建设任重道远。这是学术界和产业界致力攻克和亟待解决的另一个难题。

2 基于区块链的农产品供应链溯源未来研究趋势

从总体上看,我国现有的农产品供应链存在着农产品非标准化、质量波动大、地理区域高度分散等特性,使得溯源系统的建立尤为困难。同时,我国目前实行的是农产品分段式治理,生产阶段归农业部门管理,销售阶段归市场监管部门管理,因此多年来溯源系统无法形成有效的闭环。另外,由于农产品的特殊性,造成农产品的质量损失不可逆,且难以量化,使得农产品质量追溯的难度和成本急剧上升。

针对上述我国农产品供应链的特点,结合作者在进行国家自然科学基金重点项目与京东集团合作开展的“京东农场”示范工程建设实践过程中累积的经验,作者发现:要建立可信可靠的农产品供应链溯源系统,需要设计合适的商业模式。具体而言,针对分散的小农模式的特色农产品供应链溯源,可以建立由政府主导的、以物流或销售企业为核心的、农民生产合作社/农场参与的特色农产品溯源联盟,如图1所示。对于特色农产品的供应链来说,我国特色农产品通常规模化、标准化程度较高,对于此类农产品建立由政府主导的“高度开放、共享共用、通识通查”的农产品溯源联盟,既可以纵向地覆盖特色农产品供应链参与方,又可以横向地整合本地农产品企业,扩大联盟规模,实现资源共享、降低平均投入成本同时,在溯源联盟中加入了监管机构、检测机构、执法机构做区块链的节点对溯源数据进行记录和监督检查,形成政府背书,规范农产品供应链的整个运作过程。对于分散的小农模式供应链来说,以物流或者销售企业为核心,基于合作社或农场整合前端农民实现标准化生产和信息采集,同时引入农业部门、市场监管部门以及检验检疫机构等政府部门作为背书节点,建立“企业-政府各部门-社会”的共建体系,实现生产和流通过程的标准化以及闭环溯源系统。基于上述“优质优价、价值共创”的商业模式,通过基于区块链的溯源系统能有效地将产品的品质特性传递给顾客,建立顾客信任,吸引愿意为优质农产品支付优价的顾客,提升供应链的整体效益,从而一定程度上缓解了由农产品的低价格和物联网、区块链系统的高造价带来的收支差异问题。此外,有针对性地政府补贴、吸引第三方机构投资农产品溯源体系基础设施建设,也可以为解决这一难题提供帮助。

虽然作者及研究团队已经积累了一定的经验,但是实践过程中基于区块链的农产品供应链溯源系统仍然面临着“如何建”和“如何查”这两个关键问题。为此,学术界和产业界应立足于我国农产品供应链的独特特点,集成物联网和区块链技术,设计通用的农产品溯源标准,构建从发现问题(感知、识别)、到查找问题(追寻)、到确定问题(问责)、再到解决问题(治理)的新型全功能农产

品供应链溯源系统. 具体而言, 结合已有研究, 可以从理论方法研究和应用实践两个角度共同入手

(如图 2 所示) 综合集成区块链、物联网、大数据和人工智能等相关技术方法开展研究.

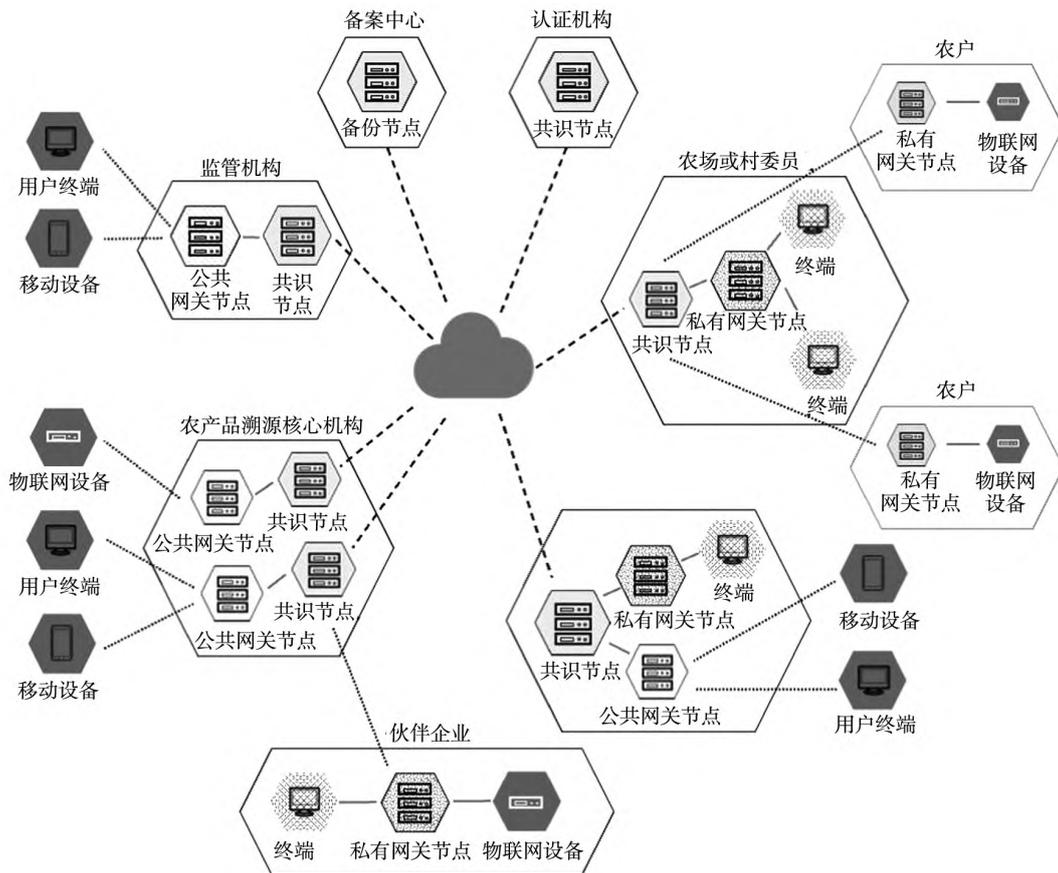


图 1 基于区块链的农产品供应链溯源联盟架构示意图

Fig. 1 Framework of the alliance of blockchain-based traceability systems for agri-food supply chains

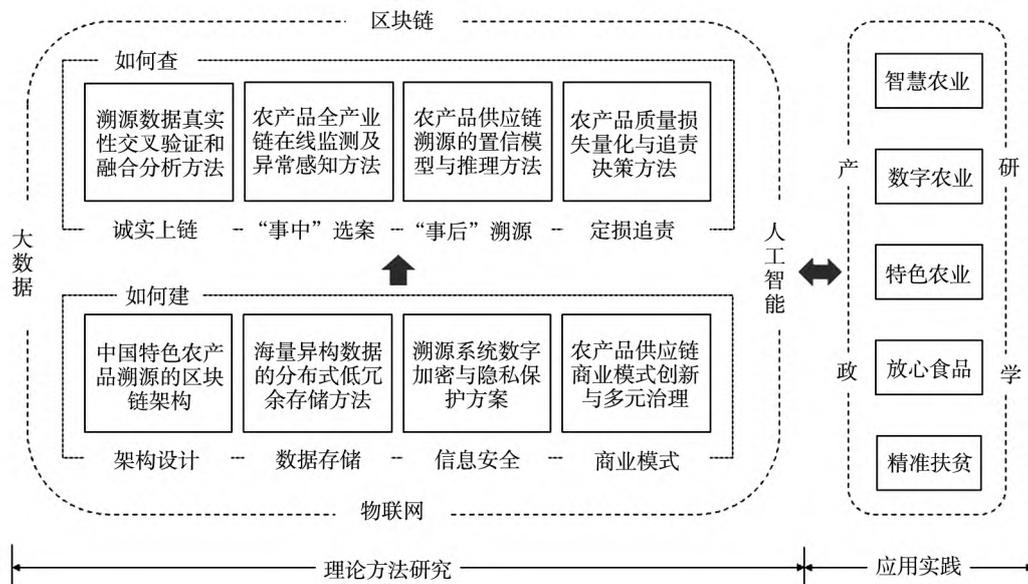


图 2 基于区块链的农产品供应链溯源的未来研究工作

Fig. 2 Future research of blockchain-based traceability systems for agri-food supply chains

首先,针对“如何建”这一难题,需要研究以下四类关键科学问题:一是,在新的商业模式基础上,针对具体的农产品特性,构建适应于中国分散式个体农户和大规模消费者的区块链溯源架;二是,针对农产品供应链的链条长、周期长、所涉及的溯源数据要素多的特点,构建区块链的农产品供应链溯源系统海量异构数据的低冗余存储方法;三是,针对农产品供应链中不同主体及信息需求特点制定溯源区块链中农产品数据的保密属性,研究适用于农产品供应链溯源的数据加密机制以及可追责的农产品区块链数据的隐私保护方案;四是,农产品供应链商业模式创新与多元治理,探讨“企业-政府各部门-社会”共建的基于区块链的农产品供应链溯源系统,以及相应的政府补贴保障和供应链多方利益分配机制。

其次,针对“如何查”这一难题,需要研究以下四类关键科学问题:一是,针对上链数据真实性验证问题,结合农产品供应链多参与方提供的多源数据,设计可信的溯源数据真实性交叉验证和融合分析方法;二是,针对农产品质量安全“事中”选案难题,结合证据理论、大数据和人工智能技术,研究农产品全产业链在线监测及异常感知方法;三是,针对农产品质量安全“事后”溯源难题,研究农产品供应链溯源的置信模型与推理方法,形成“信息链-证据链-信任链”为主线的农产品质量置信溯源方法;四是,针对农产品质量安全事故追责难题,研究农产品质量损失量化方法,以及农产品质量安全责任主体追责决策方法。

最后,在应用实践层面,中国是一个农业大国和人口大国,“质量兴农”是我国长期发展的战

略,区块链和物联网等技术是我国“新基建”发展政策中的核心部分,而京东、阿里巴巴、腾讯等高新技术企业已经走在世界前列开启了智慧农业的相关业务实践,学者们应该借助这一优势,面向我国重大需求开展“政、产、学、研”多方合作,扎根中国大地,解决中国难题,推动基于区块链的农产品供应链溯源系统的落地。特别是在偏远和贫困地区,可以结合地方特色农业和农产品供应链特征,探索相应的基于区块链和物联网的智慧农业新模式,进行精准扶贫,实现农产品供应链优质优价和价值共创,引领并加速我国农业向质量效益型的智慧农业发展。

3 结束语

本研究详细分析了我国利用区块链技术实现农产品供应链溯源过程中所面临的机遇与挑战,结合链上信息泄露和溯源信息造假这两个管理实践难题,对区块链技术与应用、信息安全隐私保护以及信任的传递与融合三个方面研究进行综述,总结提炼出“如何建”和“如何查”这两个核心问题及其对应的关键科学问题。相关研究有利于物联网与区块链、人工智能与机器学习等技术的系统集成以及大数据、信任传递与融合理论的交叉集成,催生基于区块链的农产品供应链置信溯源新理论方法,有利于学科交叉和新学科的诞生,具有重要的理论意义。同时,“政产学研”结合,积极推动示范工程建设,将引领中国“包产到户”的分散式农业逐步向质量效益型的现代农业发展,推进国家质量兴农战略向前发展,为解决中国智慧农业发展难题,具有重要现实意义。

参考文献:

- [1]中国政府网. 农业农村部等七部门联合印发《国家质量兴农战略规划(2018—2022年)》[EB/OL]. [2019-02-20]. http://www.gov.cn/xinwen/2019-02/20/content_5367181.htm.
Website of Chinese Government. Seven departments including the Ministry of Agriculture and Rural Affairs jointly issuing “The national strategic plan for promoting agriculture through quality (2018 - 2022)” (in Chinese) [EB/OL]. [2019-02-20]. http://www.gov.cn/xinwen/2019-02/20/content_5367181.htm. (in Chinese)
- [2]Babich V, Hilary G. Distributed ledgers and operations: What operations management researchers should know about blockchain technology[J]. *Manufacturing & Service Operations Management*, 2020, 22(2): 223-240.
- [3]Olsen T L, Tomlin B. Industry 4.0: Opportunities and challenges for operations management[J]. *Manufacturing & Service*

- Operations Management ,2020 ,22(1) : 113 – 122.
- [4]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.
- [5]汪寿阳,胡毅,熊熊,等. 复杂系统管理理论与方法研究[J]. 管理科学学报,2021 ,24(8) : 1 – 9
Wang Shouyang ,Hu Yi ,Xiong Xiong , et al. Complex systems management: Theory and methods [J]. Journal of Management Sciences in China ,2021 ,24(8) : 1 – 9. (in Chinese)
- [6]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)
- [7]Wang L ,Shen X ,Li J , et al. Cryptographic primitives in blockchains [J]. Journal of Network and Computer Applications ,2019 ,127: 43 – 58.
- [8]Qin R ,Yuan Y ,Wang F. A novel hybrid share reporting strategy for blockchain miners in PPLNS pools [J]. Decision Support Systems ,2019 ,118: 91 – 101.
- [9]Li J ,Yuan Y ,Wang F. A novel GSP auction mechanism for ranking bitcoin transactions in blockchain mining [J]. Decision Support Systems ,2019 ,124: 113094.
- [10]Xiao Y ,Zhang N ,Lou W , et al. A survey of distributed consensus protocols for blockchain networks [J]. IEEE Communications Surveys & Tutorials ,2020 ,22(2) : 1432 – 1465.
- [11]Du M ,Ma X ,Zhang Z , et al. A review on consensus algorithm of blockchain [C] // 2017 IEEE International Conference on Systems ,Man , and Cybernetics (SMC) ,IEEE ,2017: 2567 – 2572.
- [12]Hirano T ,Motohashi T ,Okumura K , et al. Data validation and verification using blockchain in a clinical trial for breast cancer: Regulatory sandbox [J]. Journal of Medical Internet Research ,2020 ,22(6) : e18938.
- [13]Khan P W ,Byun Y C ,Park N. A data verification system for CCTV surveillance cameras using blockchain technology in smart cities [J]. Electronics ,2020 ,9(3) : 484.
- [14]Li Y ,Tu Y ,Lu J , et al. A security transmission and storage solution about sensing image for blockchain in the Internet of Things [J]. Sensors ,2020 ,20(3) : 916.
- [15]Ghimire S ,Choi J Y ,Lee B. Using blockchain for improved video integrity verification [J]. IEEE Transactions on Multimedia ,2019 ,22(1) : 108 – 121.
- [16]Wei P C ,Wang D ,Zhao Y , et al. Blockchain data-based cloud data integrity protection mechanism [J]. Future Generation Computer Systems ,2020 ,102: 902 – 911.
- [17]Casino F ,Dasaklis T K ,Patsakis C. A systematic literature review of blockchain-based applications: Current status ,classification and open issues [J]. Telematics and Informatics ,2019 ,36: 55 – 81.
- [18]Aggarwal S ,Chaudhary R ,Aujla G S , et al. Blockchain for smart communities: Applications ,challenges and opportunities [J]. Journal of Network and Computer Applications ,2019 ,144: 13 – 48.
- [19]Vatankhah Barenji A ,Li Z ,Wang W M , et al. Blockchain-based ubiquitous manufacturing: A secure and reliable cyber-physical system [J]. International Journal of Production Research ,2020 ,58(7) : 2200 – 2221.
- [20]Gunasekaran A ,Yusuf Y Y ,Adeleye E O , et al. Agile manufacturing: An evolutionary review of practices [J]. International Journal of Production Research ,2019 ,57(15 – 16) : 5154 – 5174.
- [21]王宇倩,李军祥,徐敏. 区块链框架下基于前景理论的微网分布式能源协同优化 [J]. 系统工程理论与实践 ,2022 ,42(9) : 2551 – 2564.
Wang Yuqian ,Li Junxiang ,Xu Min. Collaborative optimization of distributed energy resources in microgrid based on prospect theory under the framework of blockchain [J]. System Engineering: Theory & Practice ,2022 ,42(9) : 2551 – 2564. (in Chinese)
- [22]Lu H ,Huang K ,Azimi M , et al. Blockchain technology in the oil and gas industry: A review of applications ,opportunities ,challenges , and risks [J]. IEEE Access ,2019 ,7: 41426 – 41444.
- [23]Zhang Z ,Yuan Z ,Ni G , et al. The quality traceability system for prefabricated buildings using blockchain: An integrated framework [J]. Frontiers of Engineering Management ,2020 ,7: 528 – 546.

- [24] Choi T M. Blockchain-technology-supported platforms for diamond authentication and certification in luxury supply chains [J]. *Transportation Research Part E: Logistics and Transportation Review*, 2019, 128: 17 – 29.
- [25] Iyengar G, Saleh F, Sethuraman J, et al. Economics of permissioned blockchain adoption [J]. *Management Science*, 2023, 69(6): 3415 – 3436.
- [26] Dong L, Jiang P, Xu F. Impact of traceability technology adoption in food supply chain networks [J]. *Management Science*, 2023, 69(3): 1518 – 1535.
- [27] Sodhi M M S, Seyedghorban Z, Tahernejad H, et al. Why emerging supply chain technologies initially disappoint: Blockchain, IoT, and AI [J]. *Production and Operations Management*, 2022, 31(6): 2517 – 2537.
- [28] Di Vaio A, Variante L. Blockchain technology in supply chain management for sustainable performance: Evidence from the airport industry [J]. *International Journal of Information Management*, 2020, 52: 102014.
- [29] Choi T M, Wen X, Sun X, et al. The mean-variance approach for global supply chain risk analysis with air logistics in the blockchain technology era [J]. *Transportation Research Part E: Logistics and Transportation Review*, 2019, 127: 178 – 191.
- [30] Rahmanzadeh S, Pishvaei M S, Rasouli M R. Integrated innovative product design and supply chain tactical planning within a blockchain platform [J]. *International Journal of Production Research*, 2020, 58(7): 2242 – 2262.
- [31] Wang Z, Zheng Z, Jiang W, et al. Blockchain-enabled data sharing in supply chains: Model, operationalization, and tutorial [J]. *Production and Operations Management*, 2021, 30(7): 1965 – 1985.
- [32] Yang C. Maritime shipping digitalization: Blockchain-based technology applications, future improvements, and intention to use [J]. *Transportation Research Part E: Logistics and Transportation Review*, 2019, 131: 108 – 117.
- [33] Tang C S, Veelenturf L P. The strategic role of logistics in the industry 4.0 era [J]. *Transportation Research Part E: Logistics and Transportation Review*, 2019, 129: 1 – 11.
- [34] Chang Y, Iakovou E, Shi W. Blockchain in global supply chains and cross border trade: A critical synthesis of the state-of-the-art, challenges and opportunities [J]. *International Journal of Production Research*, 2020, 58(7): 2082 – 2099.
- [35] Zhao G, Liu S, 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.
- [36] Salah K, Nizamuddin N, Jayaraman R, et al. Blockchain-based soybean traceability in agricultural supply chain [J]. *IEEE Access*, 2019, 7: 73295 – 73305.
- [37] Kamath R. Food traceability on blockchain: Walmart's pork and mango pilots with IBM [J]. *The Journal of the British Blockchain Association*, 2018, 1(1): 47 – 53.
- [38] Xu X, Lu Q, Liu Y, et al. Designing blockchain-based applications a case study for imported product traceability [J]. *Future Generation Computer Systems*, 2019, 92: 399 – 406.
- [39] Kamilaris A, Fonts A, Prenafeta-Bold's F X. The rise of blockchain technology in agriculture and food supply chains [J]. *Trends in Food Science & Technology*, 2019, 91: 640 – 652.
- [40] Zhao G, Liu S, 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.
- [41] Aung M M, Chang Y S. Traceability in a food supply chain: Safety and quality perspectives [J]. *Food Control*, 2014, 39: 172 – 184.
- [42] Ping H, Wang J, Ma Z, et al. Mini-review of application of IoT technology in monitoring agricultural products quality and safety [J]. *International Journal of Agricultural and Biological Engineering*, 2018, 11(5): 35 – 45.
- [43] 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.
- [44] Feng T. An agri-food supply chain traceability system for China based on RFID & blockchain technology [C] // 2016 13th International Conference on Service Systems and Service Management (ICSSSM), 2016: 1 – 6, doi: 10.1109/ICSSSM.2016.7538424.
- [45] Hang L, Ullah I, Kim D. A secure fish farm platform based on blockchain for agriculture data integrity [J]. *Computers and Electronics in Agriculture*, 2020, 170: 105251.

- [46] Lin Q, Wang H, Pei X, et al. Food safety traceability system based on blockchain and EPCIS [J]. *IEEE Access*, 2019, 7: 20698 – 20707.
- [47] Li X, Jiang P, Chen T, et al. A survey on the security of blockchain systems [J]. *Future Generation Computer Systems*, 2020, 107: 841 – 853.
- [48] Yuan Y, Wang F Y. Blockchain and cryptocurrencies: Mode techniques, and applications [J]. *IEEE Transactions on Systems Man & Cybernetics Systems*, 2018, 48(9): 1421 – 1428.
- [49] 朱岩, 王巧石, 秦博涵, 等. 区块链技术及其研究进展 [J]. *工程科学学报*, 2019, 41(11): 1361 – 1373.
Zhu Yan, Wang Qiaoshi, Qin Bohan, et al. Survey of blockchain technology and its advances [J]. *Chinese Journal of Engineering*, 2019, 41(11): 1361 – 1373. (in Chinese)
- [50] Hyperledger. Hyperledger architecture working group paper [EB/OL]. <https://www.hyperledger.org/>, 2018 – 10 – 24.
- [51] Deuber D, Magri B, Thyagarajan S A K. Redactable Blockchain in the Permissionless Setting [C] // 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2019, pp. 124 – 138, doi: 10.1109/SP.2019.00039.
- [52] Shen Tu Q C, Yu J P. A blind-mixing scheme for bitcoin based on an elliptic curve cryptography blind digital signature algorithm [J]. arXiv preprint, 2015, online: <https://arxiv.org/ftp/arxiv/papers/1510/1510.05833.pdf>.
- [53] Dash. Dash is digital cash [EB/OL]. <https://www.dash.org/>, 2018 – 10 – 24.
- [54] Gaži P, Kiayias A, Zindros D. Proof-of-Stake Sidechains [C] // 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, 2019, 139 – 156, doi: 10.1109/SP.2019.00040.
- [55] Monero. About monero [EB/OL]. <https://getmonero.org/knowledge-base/about>, 2018 – 10 – 24.
- [56] Liu Z, Yang G, Wong D S, et al. Key-Insulated and Privacy-Preserving Signature Scheme with Publicly Derived Public Key [C] // 2019 IEEE European Symposium on Security and Privacy, Stockholm, Sweden, 2019: 215 – 230, doi: 10.1109/EuroSP.2019.00025.
- [57] Sasson E B, Chiesa A, Garman C, et al. Zerocash: Decentralized Anonymous Payments from Bitcoin [C] // 2014 IEEE Symposium on Security and Privacy. IEEE, 2014: 459 – 474.
- [58] 李燕, 马海英, 王占君. 区块链关键技术的研究进展 [J]. *计算机工程与应用*, 2019, 20: 113 – 123.
Li Yan, Ma Haiying, Wang Zhanjun. Research progress on key technologies of blockchain [J]. *Computer Engineering and Applications*, 2019, 20: 113 – 123. (in Chinese)
- [59] Joseph P, Thaddeus D. The bitcoin lightning network: Scalable off-chain instant payments [EB/OL]. <http://lightning-network.org/lightning-network-paper.pdf>, 2018 – 10 – 24.
- [60] 中国信息通信研究院. 区块链安全白皮书 1.0 版 [R/OL]. <http://www.caict.ac.cn/kxyj/qwfb/bps/201901/P020190111354077196849.pdf>, 2019 – 01.
China Academy of Information and Communication Technology. White paper on Blockchain security [R/OL]. <http://www.caict.ac.cn/kxyj/qwfb/bps/201901/P020190111354077196849.pdf>, 2019 – 01. (in Chinese)
- [61] Shanmugam M, Sun S, Amidi A, et al. The applications of social commerce constructs [J]. *International Journal of Information Management*, 2016, 36(3): 425 – 432.
- [62] Sun Y L, Yu W, Han Z. Information theoretic framework of trust modeling and evaluation for ad hoc networks [J]. *IEEE Journal on Selected Areas in Communications*, 2006, 24(2): 305 – 317.
- [63] Bharadwaj K K, Al-Shamri M Y H. Fuzzy computational models for trust and reputation systems [J]. *Electronic Commerce Research & Applications*, 2009, 8(1): 37 – 47.
- [64] 刘迎春, 郑小林, 陈德人. 基于信任和推荐关系的可信服务发现 [J]. *系统工程理论与实践*, 2012, 32(12): 2789 – 2795.
Liu Yingchun, Zheng Xiaolin, Chen Deren. Trustworthy services discovery based on trust and recommendation relationships [J]. *Systems Engineering: Theory & Practice*, 2012, 32(12): 2789 – 2795. (in Chinese)
- [65] Lee K C, Kang I, McKnight D H. Transfer from offline trust to key online perceptions: An empirical study [J]. *IEEE Transactions on Engineering Management*, 2007, 54(4): 729 – 741.
- [66] Richters O, Peixoto T P. Trust transitivity in social networks [J]. *Plos One*, 2011, 6(4): 1 – 14.
- [67] Kim Y A, Song H S. Strategies for predicting local trust based on trust propagation in social networks [J]. *Knowledge-*

- Based Systems ,2011 ,24(8) : 1360 – 1371.
- [68] Dempster A P. Upper and lower probability inferences based on a sample from a finite univariate population[J]. *Biometrika* ,1967 ,54(3/4) : 515 – 528.
- [69] Inglis J. A mathematical theory of evidence[J]. *Technometrics* ,1978 ,20(1) : 106.
- [70] Yang J B , Singh M G. An evidential reasoning approach for multiple-attribute decision making with uncertainty[J]. *IEEE Transactions on Systems , Man , and Cybernetics* ,1994 ,24(1) : 1 – 18.
- [71] Yang J B , Wang Y M , Xu D L , et al. The evidential reasoning approach for MADA under both probabilistic and fuzzy uncertainties[J]. *European Journal of Operational Research* ,2006 ,171(1) : 309 – 343.
- [72] Yang J B , Xu D L. Evidential reasoning rule for evidence combination[J]. *Artificial Intelligence* ,2013 ,205: 1 – 29.
- [73] Kong G , Xu D L , Body R , et al. A belief rule-based decision support system for clinical risk assessment of cardiac chest pain[J]. *European Journal of Operational Research* ,2012 ,219(3) : 564 – 573.
- [74] Fu C , Yang J B , Yang S L. A group evidential reasoning approach based on expert reliability[J]. *European Journal of Operational Research* ,2015 ,246(3) : 886 – 893.
- [75] Yang J B , Li D. Normal vector identification and interactive tradeoff analysis using minimax formulation in multiobjective optimization[J]. *IEEE Transactions on Systems , Man , and Cybernetics-Part A: Systems and Humans* ,2002 ,32(3) : 305 – 319.
- [76] Xu X , Zheng J , Yang J , et al. Data classification using evidence reasoning rule[J]. *Knowledge-Based Systems* ,2017 ,116: 144 – 151.
- [77] Liu Y , Bi J W , Fan Z P. Ranking products through online reviews: A method based on sentiment analysis technique and intuitionistic fuzzy set theory[J]. *Information Fusion* ,2017 ,36: 149 – 161.

Review of blockchain-based traceability systems for agri-food supply chains

*HU Xiang-pei*¹ , *DU Mu*^{1*} , *KONG Xiang-wei*² , *ZHU Shan*¹ , *ZHANG Yuan-kai*³

1. School of Economics and Management , Dalian University of Technology , Dalian 116024 , China;

2. School of Management , Zhejiang University , Hangzhou 310058 , China;

3. School of Economics and Management , Beihang University , Beijing 100191 , China

Abstract: Supply chains of agricultural products in China are man-machine complex systems , characterized by multi-stage , multi-link , and dynamic scalable network chains with multi-stakeholder participation. Hence , the blockchain traceability system is facing a series of challenges , such as privacy protection , information security , and tracing data reliability. Motivated by the real-world demand and application challenges , the paper reviews related literature from three aspects: 1) blockchain technologies and applications , 2) blockchain-based privacy protection and information security in the agri-food supply chain , and 3) trust transitivity and fusion. Two core issues in building a blockchain-based traceability system for the agri-food supply chains , i. e. , “how to build” and “how to detect” , are proposed. Moreover , four research questions for each issue are proposed from the perspective of management science , and future research trends are discussed. Finally , suggestions are put forward for further deployments and applications.

Key words: agri-food supply chain; blockchain; quality traceability; privacy protection and information security; trust transitivity and fusion