基于区块链的农产品安全可信溯源应用研究

高阳阳 吕相文 袁 柳 李 勐
(中国电子科技集团公司电子科学研究院 北京 100041)

摘 要 传统中心化溯源系统信任感低且安全性受限,区块链技术具有去中心化、分布式网络、强安全加密机制和记录公开透明不可篡改的特点,能够克服集中式溯源系统的诸多缺点。通过将区块链技术应用于解决品牌农产品当前溯源的痛点问题,形成集农业物联网、智能全景监控、智能防伪和区块链技术于一体的强信任溯源应用体系。将品牌农产品关键生命周期信息上链,采用多方验证参与的模式,基于区块链分布式存储、点对点传输、共识、记录不可删除不可篡改等技术特性,构建整个品牌农产品的全产业链关键信息不可篡改不可伪造的强信任背书追踪溯源能力。通过实验验证品牌农产品链的信息上链及其响应性能,结果表明基于区块链的溯源应用体系具有高可用性、安全性和可信度。

关键词 区块链 安全 可信 溯源 强信任 农产品

中图分类号 TP3 **文献标志码** A DOI:10.3969/j.issn.1000-386x.2020.07.054

APPLICATION OF BLOCKCHAIN-BASED TRUSTED TRACEABILITY OF AGRICULTURAL PRODUCTS

Gao Yangyang Lü Xiangwen Yuan Liu Li Meng
(*China Academy of Electronics and Information Technology*, *Beijing 100041*, *China*)

Abstract Traditional centralized traceability system has low trust and limited security. Blockchain technology has the characteristics of decentralized, distributed network, strong security encryption mechanism and open and transparent records, which can overcome many shortcomings of centralized traceability system. By applying Blockchain technology to solve the pain point of brand agricultural products traceability, a strong trust traceability application system integrating agricultural Internet of things, intelligent panoramic monitoring, intelligent anti-counterfeiting and Blockchain technology is formed. The key life cycle information of brand agricultural products was put on the chain, and the multi-party verification and participation mode was adopted. Based on the characteristics of Blockchain distributed storage, point-to-point transmission, consensus and non-tampering, we built a strong trust endorsement traceability that could not be tampered with and forged for the whole industrial chain key information of the brand agricultural products. The information chain and its response performance of brand agricultural products chain were verified by experiments. The results show that the traceability application system based on Blockchain has high availability, security and credibility.

Keywords Blockchain Security Trust Traceability Strong trust Agricultural products

0 引 言

品牌农产品溯源技术是保障品牌信誉和消费者权益的关键技术之一。然而,目前市面上存在这样的乱象:消费者能买到的“品牌农产品”远远超过实际产量,且产品定价混乱,使得消费者难以分辨产品真假,严重影响品牌价值增长和信誉形象。文献[1-2]从溯源标识数据模型以及技术应用角度进行了溯源应用研究。文献[3-4]从可信机制及管理平台方面进行了研究。文献[5-7]针对新方法、算法和应用方面进行了分析。文献[8-9]针对新模式和新的溯源验证

收稿日期:2019-04-28。**高阳阳**,工程师,主研领域:计算机网络,网络空间与大数据,网络空间安全。**吕相文**,高工。**袁柳**,工程师。**李勐**,工程师。

联盟进行了探索。本文研究基于农业物联网、智能全景监控、智能防伪和区块链技术的去中心化溯源应用体系,将品牌农产品从种植、仓储、加工到销售等全产业链进行追溯应用,在种植环节植入相关传感器,实时传输至可追溯系统,实现农田墒情智能控制、仓储环节全自动温湿度控制、加工环节可视化、销售环节可追踪等能力,通过商品追溯码在平台上验证品牌农产品可信来源产业链信息,基于区块链的溯源系统提升了溯源的安全性、稳定性和可信度。

1　需求分析

1.1　溯源系统痛点分析

(1) 品牌农产品溯源信任感缺失。传统中心化溯源系统需要使用具有公信力的工具对溯源对象进行真伪辨别。防伪标签不能物理地捆绑产品,同时普通标签可以很容易地被复制。溯源信任感需要对全产业链关键环节进行追溯,例如,为了追踪品牌农产品进行溯源,如果能将农产品产业链中种植生产环节、相关生产和销售环节关键细节数据等进行如实记录,对于提高追踪溯源可信度具有重要作用。但是,传统中心化溯源信息信任感缺失,无多方参与验证,导致信任背书主体信任感不足。

(2) 传统中心化溯源易篡改。传统溯源系统是中心化系统,当溯源信息被记录到中心化节点的信息系统数据库中,集中式存储的数据可能被黑客攻击,导致数据丢失和损坏严重等问题。此外,中心化集中式溯源系统数据还极有可能遭受来自人为恶意的修改或者操作。在传统的验证中心化模式下,数据存储在各自不同的平台上,容易被篡改,导致真假难辨,进而威胁到整个溯源系统数据的真实性,影响后续防伪验证环节的用户体验。

(3) 传统中心化溯源系统性能欠佳。目前,在传统中心化溯源体系下,整个产业链中存在着严重的信息孤岛问题。由于整个产业链中存在多个信息系统,信息系统归属和权限不同,导致它们彼此之间交互变得不易,从而造成繁琐的信息核查验证。特别是当产业链中间环节长而复杂时,很难掌握各个节点的具体可控性,为了弥补这个问题,将会增加额外的诸多核验和重复检查工作量。

1.2　区块链适配溯源的关键技术特点

鉴于以上痛点问题,本文将区块链技术用于解决目前农产品追踪溯源领域中遇到的现实问题。基于区块链的溯源应用体系旨在提升防伪存证溯源和真实性,保障品牌农产品质量和安全,为树立品牌信誉提供强信任技术背书。区块链技术可用于溯源应用体系的关键技术特点包括:

(1) 在系统节点彼此不信任的场景下实现去中心化的强信任背书能力。区块链系统技术本身保证了其真实性和可信任,并且不只是依靠外部公信力工具,而是整个系统都在提供信任背书,从技术上提升可信度。

(2) 分布式网络架构,不存在单点故障,整体技术架构方面具有强稳定性、可靠性和可持续性。

(3) 强安全加密机制,共识机制达成分布式一致性时不要求第三方进入,通过技术手段,实现整个去中心化系统参与方的协同合作。

(4) 区块链上记录的数据具有只能增加不能修改的技术特征,这决定了区块链信息的不可删除性和不可篡改性。

2　区块链溯源优势

鉴于中心化溯源系统缺乏追踪溯源信任感的问题,通过区块链多方参与验证,多方共同维护同一个账本的模式,争取与品牌农产品产业链关键环节众多参与者形成联盟。随着联盟参与方数量的增加,共同维护的数据越多,越能够带来更多的数据信任背书主体,为消费者提供更强的信任感支撑。

针对中心化溯源易篡改的问题,区块链技术本身具有去中心化特性通过分布式网络架构克服了中心化系统的各种缺点。同时,区块链技术在溯源系统中的应用也可以避免人为恶意或者意外的数据丢失和误操作等问题。此外,系统多参与方共同维护同一账本的特性,有助于打破不同系统之间存在的信息孤岛问题。最后,区块链技术本身还能够带来支付即结算的清算能力,减少多方重复对账所带来的诸多问题和相应成本。

区块链技术可以保证数据上链后的真实性、不可删除性与不可篡改性,为了保证上链前数据的真实性和准确性,可在追踪溯源系统中综合运用多种技术手段。例如,当品牌农产品喷码记录上链时,我们可以在包装箱中放置一个绑有电子标签的全球定位系统(GPS)装置,用以跟踪品牌农产品物理位置信息,可跟随该品牌农产品信息上链记录实时流转的 GPS 定位信息,从而保障该农产品在区块链上记录的地理位置的真实性,给予商品上链前线下真伪鉴定的方式和手段,从而在源头上夯实溯源信息真实性。

综上,区块链技术应用于品牌农产品追踪溯源场景,可以在保障品牌农产品整个产业链关键环节信息数据记录存入区块链后,整个参与区块链的主体都能跟踪看到各个环节的关键信息,而且信息不会被人为篡改。根据链上存储的信息可以很容易地追溯到每个信息数据被记入的关键环节点,并且避免了单点数据损坏的威胁。区块链技术为品牌农产品溯源领域的问题带来了新的解决方案,为产业链各关键环节带来了更多的信息价值。基于区块链的溯源系统就是去中心化溯源系统,同时,将农业物联网、智能监控技术、区块链技术和智能防伪技术有机结合起来,利用区块链在追踪溯源领域的技术优势,解决产业链上的信息不透明问题,从源头上解决品牌农产品的可追踪溯源信任问题,保护消费者的利益,同时提供对品牌方品牌价值的强信任背书的技术支撑。

基于区块链的农产品溯源优势包括将品牌农产品种植、生产、物流、销售等全产业链关键环节数据上链,保证数据真实不可篡改,实现基于区块链溯源系统的强信任背书。品牌农产品生产方可以利用互联网身份标识相关技术,通过品牌农产品溯源链跟踪记录其生产的农产品信息,在区块链溯源系统上完成认证后,生成区块链品牌农产品生产信息链,形成透明和安全的记录。记录在区块链溯源系统中的生产信息同时能够帮助零售方管理不同店面中的品牌农产品的生产日期、上架日期和来源等。消费者可以通过区块链提供的分布式溯源应用,对品牌农产品从种植到购买的整个产业链进行溯源查验,便捷地查询到不可篡改的商品全产业链溯源信息,通过品牌农产品产业链可信联盟参与的基于区块链的溯源系统可以保障品牌及消费者利益,树立品牌信誉,同时,消费者可以购买到安全、真实的品牌农产品。

3 应用实现

3.1 应用体系

区块链溯源一体化应用体系如图 1 所示,主要包括农业物联网设备层、网络层、溯源链平台和智慧应用层。其中农业物联网结合种植、仓储、加工和销售实际产业环境需求,在关键节点部署农业物联网传感器,主要包括:土壤墒情、农田水位、雨量、风力、光照、气压、温湿度等传感器,以及自主研发的全景监控设备。其中,智能传感器采集信息通过部署的物联网网关传到系统中,全景监控设备通过交换机接入到网络中传输到后台系统服务器。

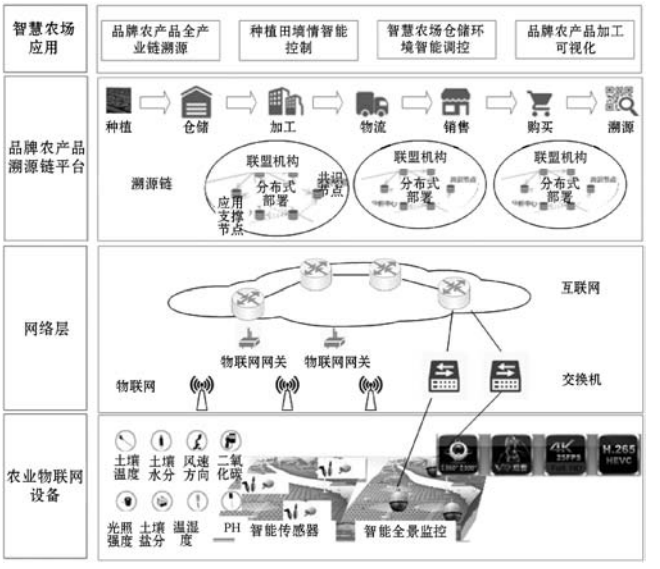

图 1 品牌农产品溯源应用体系架构

同时,利用区块链技术、物联网智能设备、全景监控和智能防伪技术,可以融合区块链技术和农业物联网所需智能硬件设备部署。在品牌农产品信息记入溯源链平台前,用机器代替人力对农产品信息进行校验,减少道德风险,确保品牌农产品信息的真实性,针对品牌农产品关键环节如种植、仓储、加工和销售等的信息进行采集验证上链。基于区块链分布式存储、点对点传输、共识和不可篡改等,构建整个品牌农产品的全产业链信息不可篡改、不可伪造的强信任追踪溯源应用体系。基于区块链溯源应用,每件品牌农产品都有了身份证,采用智能防伪技术,实现品牌农产品的开封即销毁而且不可复制。

品牌农产品生命周期强溯源平台如图 2 所示,包括物联网系统、视频监控系统、去中心化溯源系统三个部分。通过虚实映射结合的方式,将产品生命周期关键信息进行验证记录,通过多方参与,共同保障产品的强信任度。

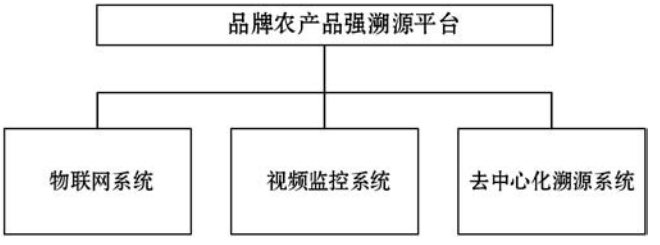

图 2 品牌农产品强溯源平台组成系统示意图

物联网系统实现品牌农产品生长环境信息自动采集,对应的传感设备可包括但不限于:多参数气象传感器、光合有效辐射传感器、水位传感器、土壤水分温度电导率传感器和土壤养分含量测量仪。数据采集传输处理包括:数据处理平台软件、无线数据采集模块和无线智能网关。集成的物联网系统可以全维度采集监测农产品生长环境信息,能够预测周围区域的小气候,预

测内容丰富:气温、空气相对湿度、风速、风向、气压和降雨等。

视频监控系统采用全景监控和普通监控结合的模式。全景监控采用智能全景监控,对比其他监控方案,监控视角广,水平 360 度,垂直 360 度,广域范围,1 500 万像素 360°全景网络监控采用一体化设计模式,方便农产品种植环境快速安装,输出最高分辨率可达 4 k(4 096 ×2 048)画质,可以针对重要细节更加清晰呈现。

去中心化溯源应用系统依赖于区块链上数据不可删除、不可篡改和不可伪造的重要特性,建立强信任品牌农产品溯源应用体系。溯源系统主要包括农产品仓储追溯、生产加工追溯、销售溯源、视频监控、农产品溯源链及其软件管理系统功能。

去中心化溯源应用系统关键技术架构如图 3 所示,它建立在区块链 3.0 架构的基础上。品牌农产品溯源链提供多种客户端访问形式,经接入网关认证,可以形成按照溯源既定规则进行的弱信任或互不信任的多参与方进行协同合作,品牌农产品区块链溯源采用联盟链,同时能够提供图灵完备的智能合约平台。

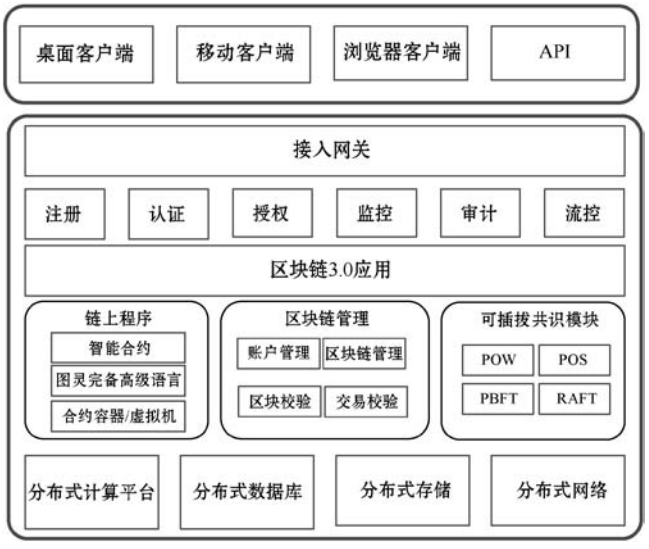

图 3　系统关键技术架构图

3.2　区块链溯源应用系统流程

区块链溯源应用系统通过为品牌农产品赋予独一无二的“身份证”让农产品从种植开始直到最终被消费者购买,全产业链关键环节信息都会被存证在区块链上。品牌农产品独一无二的“身份证”即拆即毁、不可被复制,确保消费者溯源验证信息未被篡改。

数据上链,对于农产品品牌方来说,通过终端设备,使用区块链技术,品牌农产品溯源系统将品牌农产品数据记入溯源区块链,并通过哈希函数和椭圆曲线 ECC 非对称加密算法等对数据进行加密和验证,确保整个区块链的参与方能够透明地查看各个环节信息,并且存证信息不会被人为篡改。

对于消费者来说,在选择购买品牌农产品时,可通过微信扫一扫溯源二维码等便捷易用的方式,查看追溯验证这件品牌农产品从种植、生产、包装、运输、报检、第三方检验等关键环节全过程认证信息,从而利用溯源系统提升品牌产业链信息的真实溯源,增强品牌信任感。

基于区块链的品牌农产品溯源链可进一步应用于防伪、溯源、防窜货及控价、微信互动、大数据收集分析决策、区块链和产业链可信溯源等多个应用交叉领域。

利用高科技进行品牌农产品溯源,使品牌农产品全产业链数据成为区块链上的可信环节,不仅可以进一步推动品牌农产品销售,也是集农业物联网、智能全景监控、智能防伪和区块链技术的强信任背书溯源应用体系的重要组成部分。

4　仿真实验

4.1　实验环境

实验环境为 Linux 操作系统,硬件部署环境为 Intel(R) Xeon(R) CPU E5-2680 v3 48 核、64 GB 内存、2.2 TB 硬盘,品牌农产品溯源链实验软件环境、轻量级虚拟机和测试数据。

4.2　实验方法

本实验针对品牌农产品信息上链和响应时间性能进行验证,从上链信息和响应时间来评估溯源系统的高可用性和稳定性。实验以不同的上链信息数据规模和不同的请求频次对应的上链响应时间为评估要素,验证信息上链的可用性和稳定性。

4.3　实验结果

在溯源信息量规模固定的情况下,采用不同的频率进行数据上链,对应的上链响应时间变化如图 4 所示,随着频率增大,响应时间减少,单位信息请求平均响应时间也在不断减少。

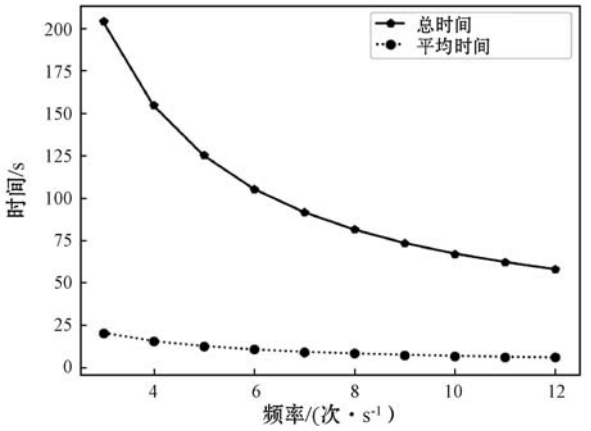

图 4　不同频率对应响应时间变化

在溯源信息上链频率固定的情况下,针对不同的溯源信息量规模,上链响应时间变化如图 5 所示,随着信息量规模增大,单位信息响应时间基本保持不变。

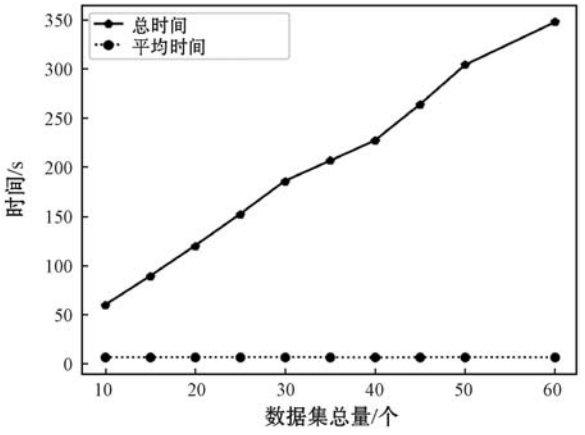

图 5 不同数据量对应响应时间变化

由实验结果可以看出,基于区块链的农产品安全可信溯源应用系统在不同规模溯源信息及不同请求频率下具有高可用性和稳定性,单位信息上链响应平均时间在秒级,具有可扩展性。

5 结 语

本文研究了将区块链技术应用于品牌农产品溯源的一体化应用体系,解决中心化溯源系统信任度低和系统安全的问题,品牌农产品溯源链分布式、不可篡改和共识验证等特性提升了系统的安全性和可信任度。从溯源信息上链和响应时间方面对去中心化溯源系统进行了仿真,结果表明基于区块链的强信任溯源系统具有高可用性和稳定性,且在分布式溯源数据上链可扩展性等方面表现良好。下一步将通过对溯源链细节进行优化,提升不同场景下的系统整体性能表现。

参 考 文 献

[1] 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.

[2] 何蒲,于戈,张岩峰,等. 区块链技术与应用前瞻综述[J]. 计算机科学,2017,44(4):1 - 7,15.

[3] 李静元,范祥辉,王颖. 基于区块链的共享经济隐私保护机制的设计[J]. 计算机应用与软件,2019,36(1):296 - 301.

[4] 杨慧琴,孙磊,赵西超. 基于区块链技术的互信共赢型供应链信息平台构建[J]. 科技进步与对策,2018,35(5):21 - 31.

[5] 钱卫宁,邵奇峰. 区块链与可信数据管理:问题与方法[J]. 软件学报,2018,29(1):150 - 159.

[6] 宋焘谊,赵运磊. 区块链共识算法的比较研究[J]. 计算机应用与软件,2018,35(8):1 - 8.

[7] 陶启,崔晓晖,赵思明,等. 基于区块链技术的食品质量安全管理系统及在大米溯源中的应用研究[J]. 中国粮油学报,2018,33(12):110 - 118.

[8] 宋远方,冯绍雯,宋立丰. 互联网平台大数据收集的困境与新发展路径——基于区块链理念[J]. 中国流通经济,2018,284(5):5 - 13.

[9] 紫琳. 中国首个安全食品区块链溯源联盟成立[J]. 中国食品,2018(1):173.

(上接第 312 页)

性设计将会更易于本文方案的实际应用,尤其是对于现在应用广泛的区块链技术。下一步,我们将会注重研究群签名的实际应用。

参 考 文 献

[1] Chaum D, Heyst E V. Group signatures [C]//Advances in Cryptology—EUROCRYPT'91, 1991: 257 - 265.

[2] Camenisch J, Stadler M. Efficient group signature schemes for large groups [C]//Advances in Cryptology—CRYPTO'97, 1997: 410 - 424.

[3] Camenisch J, Michels M. A group signature scheme based on an RSA-variant [EB/OL]. 1998. Http://citeseer. nj. nec. com/camenisch98group. html.

[4] Ateniese G, Camenisch J, Joye M, et al. A practical and provably secure coalition-resistant group signature scheme, Advances in Cryptology—CRYPTO 2000, 2000: 255 - 270.

[5] 李凤银,禹继国,鞠宏伟. 一种基于 RSA 的群签名方案[J]. 计算机工程与设计,2006,27(16):2955 - 2957.

[6] 姜燕. 基于 RSA 的群签名方案的缺陷及改进方案[J]. 计算机工程与设计,2008,29(7):1655 - 1657,1671.

[7] 朱莹,蔡光兴. 一种基于 RSA 群签名方案的安全性分析及改进[J]. 湖北工业大学学报,2009,24(1):68 - 70,73.

[8] 白永祥. 一种高效群签名方案的设计与分析[J]. 通信技术,2015,48(2):214 - 218.

[9] 于璇,侯书会. 一种高效安全的群签名方案[J]. 通信技术,2018,51(2):413 - 418.

[10] 张晓琳. 前向安全的群签名研究[D]. 青岛:青岛大学,2016.

[11] 韩嫣. 具有前向安全性的动态属性群签名研究[D]. 武汉:武汉理工大学,2017.

[12] 王硕,程相国,陈亚萌,等. 前向安全的群签名方案[J]. 青岛大学学报(自然科学版),2017,30(3):35 - 39.

[13] 王越,程相国,王戌琦. 基于双线性对的密钥隔离群签名方案研究[J]. 信息网络安全,2018,18(6):61 - 66.

[14] Boneh D, Lynn B, Shacham H. Short signatures from the weil pairing[C]//7th International Conference on the Theory and Application of Cryptology and Information Security,2001: 514 - 532.