doi:10.3772/j.issn.2095-915x.2018.03.002

基于区块链的农产品溯源系统

张延华[1,2] 杨兆鑫[1] 杨睿哲[1,2] 金凯[1] 林波[1] 司鹏搏[1,2]

1. 北京工业大学信息学部 北京 100124;
2. 北京未来网络高精尖创新中心 北京 100124

摘 要 近年来，随着消费者对农产品质量的关注度提高，可靠、可信农产品溯源技术也日益得到重视。本文提出一种依托智慧农业的区块链溯源框架，通过融合无线传感器网络、智能前端 APP、数据库以及二维码标签扫描拍照等技术，基于以太坊环境设计实现了一个农产品溯源系统。农户接入系统之后，数据采集前端将数据存储至区块链系统中，利用区块链本身具备的去中心化、不可篡改、安全加密等特点，结合后台管理数据库以及溯源二维码为消费者提供安全、可靠、真实的农产品溯源信息。系统经过实地部署和应用测试，实现了农产品从生产采摘直到消费者餐桌的全程溯源。

关键词： 区块链；以太坊；农产品溯源

中图分类号： G35

开放科学（资源服务）标识码（OSID）

Traceability System of Farm Produce Based on Blockchain

ZHANG Yanhua[1,2] YANG Zhaoxin[1] YANG Ruizhe[1,2] JIN Kai[1] LIN Bo[1] SI Pengbo[1,2]

1. Faculty of Information Technology, Beijing University of Technology, Beijing 100124, China;
2. Beijing Advanced Innovation Center for Future Internet Technology, Beijing 100124, China

Abstract In recent years, with the increase of consumers' attention to the quality of agricultural products, reliable and reliable traceability technology of agricultural products has been paid more attention.

基金项目： 国家自然科学基金资助项目（61571021）；北京工业大学基础研究基金项目(040000546317525)。

作者简介： 张延华（1960–），教授，研究方向：信号及信息处理、智慧无线通信网络方面的研究，E-mail: zhangyh@bjut.Edu.cn；杨兆鑫（1993–），博士研究生，研究方向：区块链技术与数据挖掘技术；杨睿哲（1982–），讲师，研究方向：无线通信技术与移动边缘计算技术等方面的研究；金凯（1994–），硕士研究生，研究方向：区块链技术及智能合约应用；林波(1993–)，硕士研究生，研究方向：移动边缘计算技术及区块链技术应用；司鹏搏（1983–），副教授，研究方向：认知无线电网络、异构无线网络、绿色通信技术方面的研究。

This paper proposed a blockchain traceability system based on smart agriculture with the integration of wireless sensor network, intelligent front-end APP, database and the QR code label scan imaging technology. The system has realized the agricultural product traceability system based on Ethereum. After farmers access to the system, data acquisition front-end data storage to blockchain system, the use of blockchain itself has the characteristics of decentralization, tamper-resistant, security encryption, combined with the backend database management and traceability QR code to provide consumers with safe, reliable and real farm products traceability information. Meanwhile, the system can guarantee the expansibility and interactivity of blockchain and other systems. After the test of the system, it can be proved that the system can realize the product traceability from the production to the consumer's table.

Keywords：Blockchain; Ethereum; traceability of farm produce

1 引言

随着社会经济的高速发展及人民生活质量的不断提高，食品及农产品的安全问题引起了社会的广泛关注。随着农业技术的不断进步，农产品的产量已经不再是困扰农业发展的瓶颈，适销对路的农产品更加需要安全可靠的质量保证。换句话说，消费者希望购买具有安全和质量保障的农产品，而生产者也希望通过渠道证明自己农产品的安全可靠性。但是，现代农业的农产品质量与安全受到生产、加工、物流等多重因素的影响，因此，建立可靠可信的农产品溯源体系是保障农产品质量安全的有效手段。

现有的大部分农产品溯源系统基于集中式数据库技术，通过条码溯源，一般只能追溯到生产企业，未深入到全程质量安全追溯，尤其缺乏消费者所关注的生产信息及产地环境信息[1]。目前，国内主要的农产品溯源系统仍处于试点阶段，加之标准不统一，推广应用难度很大。

区块链（Blockchain）作为一种去中心化的分布式记账技术，其分布式的共识机制，公开透明的记录、传输及不可篡改的存储，为基于区块链的各种应用提供了目前最为可靠的安全性和可信度[2]。

本文基于以太坊区块链环境，融合无线传感器网络、智能前端 APP、数据库和二维码等技术构建一种新型的农产品溯源系统。该系统为每种农产品生成唯一的二维码溯源标签，通过无线传感器网络和智能前端 APP 将农产品生产过程数据（实地监测数据、图片、视频）上传至区块链记录，保证信息的公开透明且不可篡改。消费者则通过客户端 APP 读取区块链和数据库信息，获得产品从农田到餐桌的完整信息[3]。系统原型目前已经成功应用于四川富顺县以及河北张家口金坤农业。

2 区块链技术

2.1 研究背景

区块链本身是一种加密的分布式账本系统，

doi:10.3772/j.issn.2095-915x.2018.03.002

由一系列根据时间顺序生成的记录交易数据的区块（block）链接组合形成[4]。区块链主要特点如下：

首先是去中心化特点。区块链系统的宗旨是要去中心化和实现匿名，建立自己系统内公开的信任机制[5]。其信任机制建立在非对称密码学基础上，系统使用者不需要了解对方基本信息即可进行可信任的价值交换，即在没有中心机构的情况下达成共识，提高了传统网络交易的效率。

其次是交易数据公开透明的特点。区块链系统中，当新的交易数据在被共识之后存储进新的区块时，全网的节点也会将新的区块链进行同步。其意义在于，全网节点都具有完整的区块链的交易信息的备份，能够保证所有交易数据公开在全网节点中范围公开[6]。

最后是开放共识的特点。任何人在任何时间都能够通过相同的技术在区块链上录入自己的信息，而区块链在数据透明的基础上对所有交易对象都是匿名存在的，一定程度上保证了私人信息的安全性。它不依赖第三方，而是通过自身分布式节点进行网络数据的存储、验证、传递和交流，解决了传统互联网交易中基于信任而存在的第三方中介运营成本过大、网络信息安全性不高的问题[7]。

通过区块链技术形成存储的数据具有不可篡改和无法伪造的时间戳，区块链中所由的交易记录都有完整的证据链和具有高度信任的追溯环节[9]。

2.2 区块链数据格式

区块链系统中主要有两类数据载体，分别为区块 (Blocks) 和交易 (Transactions)。每个区块的组成结构如图 1 所示，包括区块头、区块体两部分[8]。其中，区块头封装当前区块头哈希值、前置区块头哈希值、时间戳、区块难度以及随机数等信息；区块体封装当前区块具体交易事项，并利用哈希函数将交易事项的文本信息转化成随机序列形式进行存储[9]。每一个区块都对应着唯一的区块高度，区块被全网认证的时间越晚，区块高度值越大。

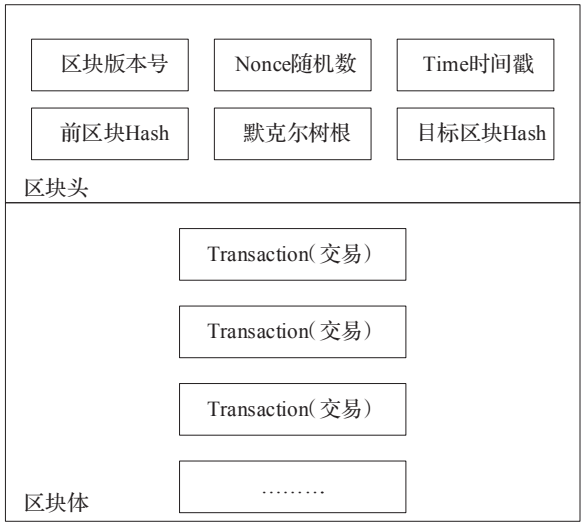

图 1 每个区块的结构图

每个交易的组成结构如表 1 所示。其中 Input 以及 From/to 字段可以由区块链的开发者自行指定，其余的字段均由区块链系统自动生成，Input 字段支持完全自定义，可以用于交易以外的额外信息存储。在该笔交易被确认之前，交易所在的区块哈希以及区块高度都不存在，当交易被确认之后才会根据实际交易区块生成数据信息。

表 1 交易信息数据段统计

	长度	描述
BlockHash	64	交易所在区块哈希地址
BlockNumber	不定长	交易所在区块的高度
Hash	64	交易的哈希地址
Input	不定长	交易的附加信息
From/to	64	交易的发起账户地址和接收账户地址

分布式网络拓扑结构使得区块链系统中的数据具有公开透明性，并实现对数据的溯源和防篡改[10]。在区块链中，数据追溯是通过时间戳服务和区块之间链式连接的设计机制实现的，并利用哈希函数加密的方式来实现数据的安全可靠性。

2.3 区块链系统架构

区块链 1.0 技术起源于虚拟货币，2008 年虚拟货币诞生，紧接着，2009 年出现了序号为 0 的虚拟货币创世区块，并与序号为 1 的区块相连形成了链，标志着区块链的诞生[3]。起源阶段的区块链基础架构模型如图 2 所示由链式结构区块、默克尔树的数据存储方式、共识机制，结合对等式网络结构及虚拟货币的激励方式组合而成[11]。

区块链2.0获得了区块链的图灵完备性[12]。节点通过简单编码实现各类数字的产生，对流通的数字资产进行精确地控制，并实现更多的非数字资产的功能产品[13]。作为区块链 2.0 技术的代表，以太坊是建立在区块链和数字资产的概念之上的一个全新开放的图灵完备的区块链平台，可以通过编写智能合约编码来创建新的数字资产，也可以通过编写智能合约的代码来创造非数字资产的功能[14]。这一复杂和灵活的智能合约的脚本语言，使得区块链能够支持宏观金融和社会系统的诸多应用[15]。目前，一般认为区块链技术正处于 2.0 模式的初期，众多如智能合约、电子商务、证券交易、股权众筹、物联网和 P2P 借贷等各类基于区块链技术的互联网金融应用相继涌现，发展前景广阔。未来区块链将更多地应用于如新型宽带网络、保险行业风险评估、艺术交易、法律公证、数字资产等生产、生活中的各个方面[16]。

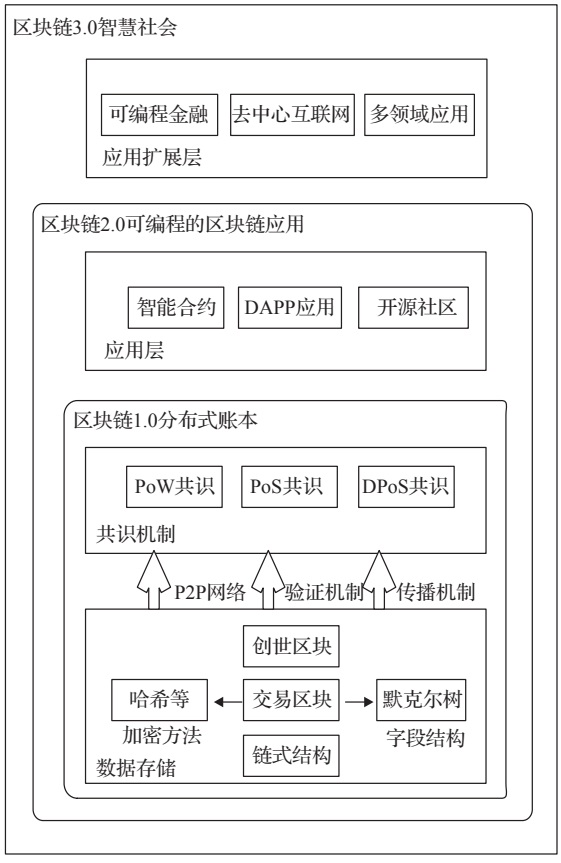

图 2 区块链的技术架构

区块链 3.0 是区块链 2.0 的一种延伸。实际上，以图灵完备的以太坊开源社区为代表的区块链 2.0 已经完全可以颠覆很多现阶段网络应用[17]。区块链 3.0 的理念在提出的时候所面

doi:10.3772/j.issn.2095-915x.2018.03.002

向的应用场景是社会的治理，也可称为可编程社会。该理念主要是在全社会对区块链普遍认可的情况下将区块链的技术引入到社会及生活中各类基础设施及日常应用中。基于区块链的社会基础设施能够以去中心化的形式配置全球资源，从而促进社会经济的发展和管理[18]。例如，社会中的民主投票选举行为以及仲裁机构的活动等，这些与信用相关的社会活动和应用在区块链去中心化的方式下进行，能够在低成本的情况下，使这些行为变得更加公开透明[19]。

3 区块链农产品溯源系统架构

3.1 研究背景

纵观国内外食品安全溯源的研究，欧盟已经要求各成员国采用国际物品协会的“全球统一编码系统”(EAN.UCC，简称统一编码)。美国加拿大等国家也具备了全国性的统一农产品追溯体系标准[18]。通过此类编码系统及溯源体系，消费者可以掌握农产品、食品的全部必要信息，一旦发生威胁人类健康的突发性食品安全事件，可以立即追踪到储运、加工和生产的各个环节，直至农产品种植或饲养的源头。相比之下，中国的农产品溯源系统仍有差距，其主要问题集中在三个方面：

（1）溯源系统缺乏统一的质量和信息标准。

现有的溯源系统主要都是通过二维码或者条码进行扫码溯源查询，不同的溯源平台对于同一类农产品所展现的溯源存储信息不统一，同样地，同一个溯源平台所展示的不同农产品对象的信息也不相同。

（2）可溯源信息量有限。

目前溯源系统使用标识条码的方法本质上属于生产商的防伪方法，仅能够证明该产品是在某个生产厂家完成的，而并没有实现农产品自身的溯源。此外，大部分超市中的溯源查询终端所展示的信息也只涉及农业生产者信息，无法实现基于该农产品的生产、加工等过程的溯源，不能够实现“从农田到餐桌”的全程信息溯源。

（3）溯源系统可靠性有待提高。

如前所述，大部分主要的溯源系统是通过中心化数据库实现，而中心化存储存在人为修改和被网络攻击的风险，使得消费者真正获取的数据真实性不能完全保证。此外，现阶段溯源系统数据录入的过程中人为的操作较多，失误率是不可控因素。

区块链技术与农产品溯源的结合能够有效改善溯源系统的不足。一方面，区块链的对等式网络节点架构能够降低数据存储系统的中心化，防止数据被篡改的风险[20]；另一方面，区块链 2.0 的图灵完备性能够支持区块链与多种已存在的业务系统交互，提高整体系统的安全可靠性；此外，通过传感器及智能采集终端等设备直接与区块链进行数据交互的方式能够保证数据来源的多样性及同一性，通过确定数据类型的需求及通信协议进而能够形成统一化的溯源体系标准。

3.2 系统架构设计

本文提出的农产品区块链溯源系统的总体架构如图 3 所示，分为数据接入层、数据服务层和用户应用层三层。数据接入层和数据服务层完成溯源系统对于农产品的数据记录和存储

功能，主要利用传感器前端网络实现数据采集和上传，并由生产过程 APP 与区块链后台通信以保证数据上载入区块链。这里，产品溯源二维码作为农产品的信息载体，贯穿于产品的生产、采摘、加工销售等关键环节的索引与记录。用户应用层则主要用来实现区块链系统与消费者之间的交互。各层级相互衔接，从而实现高效可靠的产品溯源与互动。

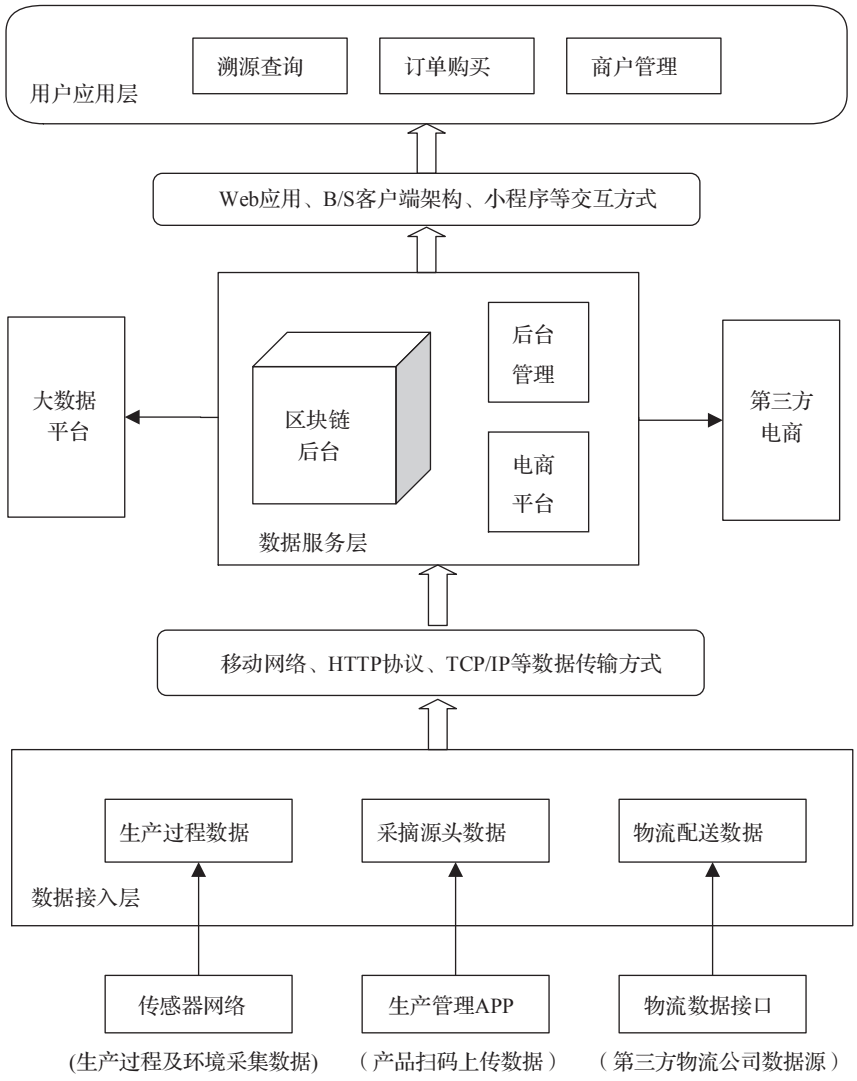

图 3 区块链农产品溯源系统整体架构图

3.3 系统业务流程分析

溯源系统的业务运行流程如图 4 所示。

系统业务运行流程如下：

（1）商户准备环节

生产商（农户）准备基础数据，电商平台为生产商提供入口，数据库中的用户表用于记录农户的基本信息，包含农场的生产品种、植株种类、生产大棚种类数量、产品属性特点等，后台管理系统与生产管理 APP 是服务器与客户端的关系，因此当农户将信息录入到后台管理系统之后，即可登录生产管理 APP 进行相应的操作。

doi:10.3772/j.issn.2095-915x.2018.03.002

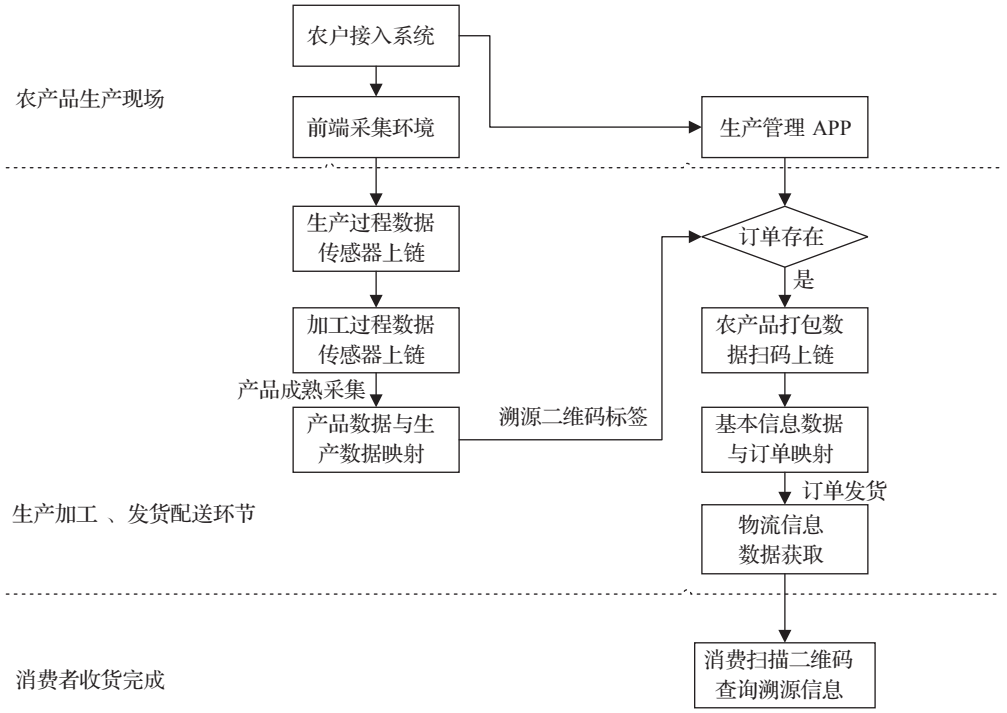

图 4 系统业务流程图

区块链系统中，每个生产商都以区块链节点的身份加入系统中每个节点负责接收其农户上传的生产、加工、包装等数据，并在区块链所有节点进行运算共识操作下将数据打包至区块内。

（2）生产发货配送环节

农产品基本数据信息通过传感器网络进行数据的记录，并通过 TCP/IP 协议上传到相应节点的区块链系统中。当生产加工过程数据上链成功后，其区块链哈希地址将转存至后台管理数据库的农产品种类数据表中进行存储。

溯源二维码包含了溯源请求查询地址以及农产品的 ID，销售时将溯源二维码贴在产品或者包装箱上，并通过生产管理 APP 选择产品种类，进行扫码和上传数据。

消费者在收货完成后可以通过扫描溯源二维码查询到产品的生产、打包、物流等全过程的数据信息以及照片和产地定位信息，实现全面的产品溯源。

3.4 溯源数据区块链存储查询方案

由于区块链当前的链式结构仅支持通过交易地址或是区块地址的查询 [21]，同时溯源数据需要与多个层级的子系统进行交互，因此数据存储方案使用区块链与数据库相结合的方式进行设计。该方案的核心是，通过区块链的交易将溯源数据进行存储，将交易地址转存至数据库与农产品 ID 建立映射，从而实现后台逻辑操作。

溯源区块链工作模式如图 5 所示。农户以区块链节点的身份加入到区块链，各农户区块链节点间形成对等式网络结构并在此基础上建立联盟链网络 [22]。通过各农户生产环境底层监测的传感器网络，产品的生产信息等数据将通过 TCP/IP 协议传输到区块链节点。每个节点由两个账户组成，第一个账户将把数据打包到一

个交易中并将交易发送给另一个账户。在传统比特币系统中，交易的确认和共识是需要由矿工来完成[23]。但在联盟链结构中，交易信息由全网各节点共同确认，保证了交易确认的效率[24]。溯源系统内数据流从生产过程到消费者查询页面的信息交换过程如图 6 所示。

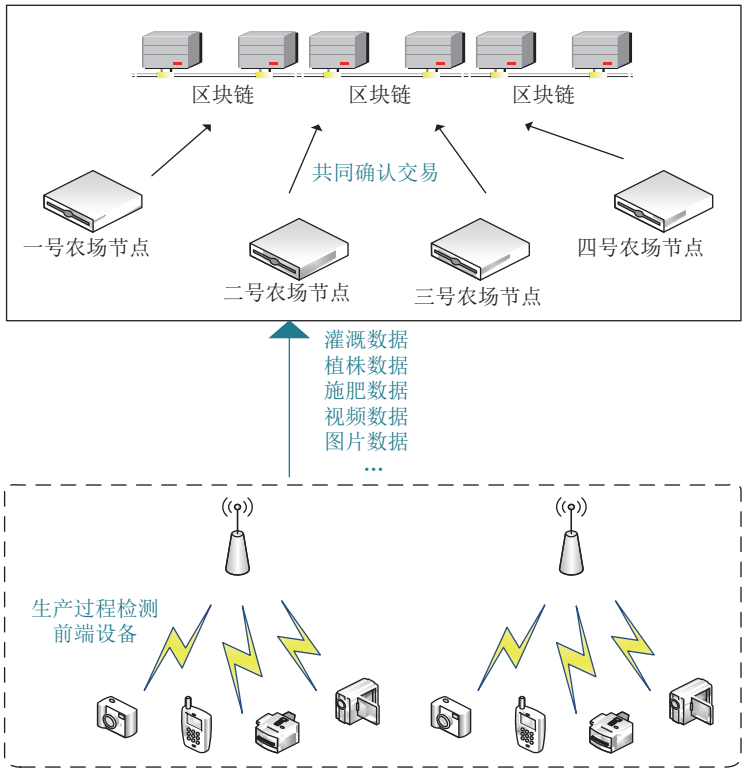

图 5 区块链多节点工作模式拓扑结构图

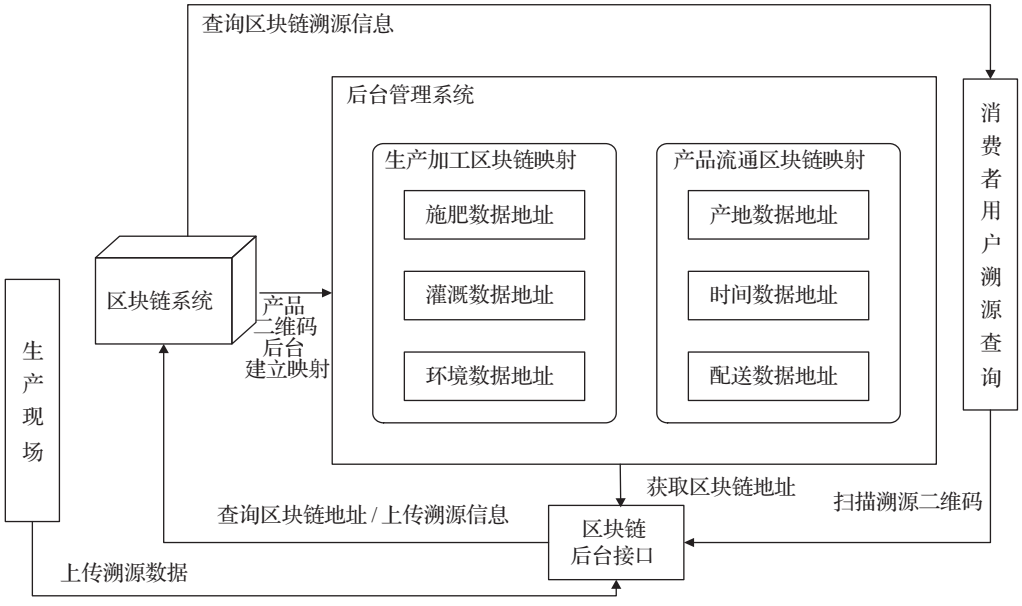

图 6 溯源系统中数据交换过程

doi:10.3772/j.issn.2095-915x.2018.03.002

系统中的数据流分为两类，即溯源信息数据和溯源请求数据，前者主要包括生产现场记录的各类生产、加工、打包等信息，需要存储到区块链的区块中；后者是溯源请求数据，主要是由消费者扫码溯源时产生，此类数据需要从后台管理系统数据库查询区块链地址并根据地址信息从区块中进行获取和展示。

4 系统设计与实现

本文基于上述区块链溯源架构，设计并实现了一个基于以太坊的农产品溯源系统，如图 7 所示。该系统由后台管理、区块链后台、生产过程录入以及溯源查询 4 个子系统组成，形成了融合电商平台、农户和消费者的，可靠可信的开放式农产品溯源平台。目前，该平台已经正式上链运营。

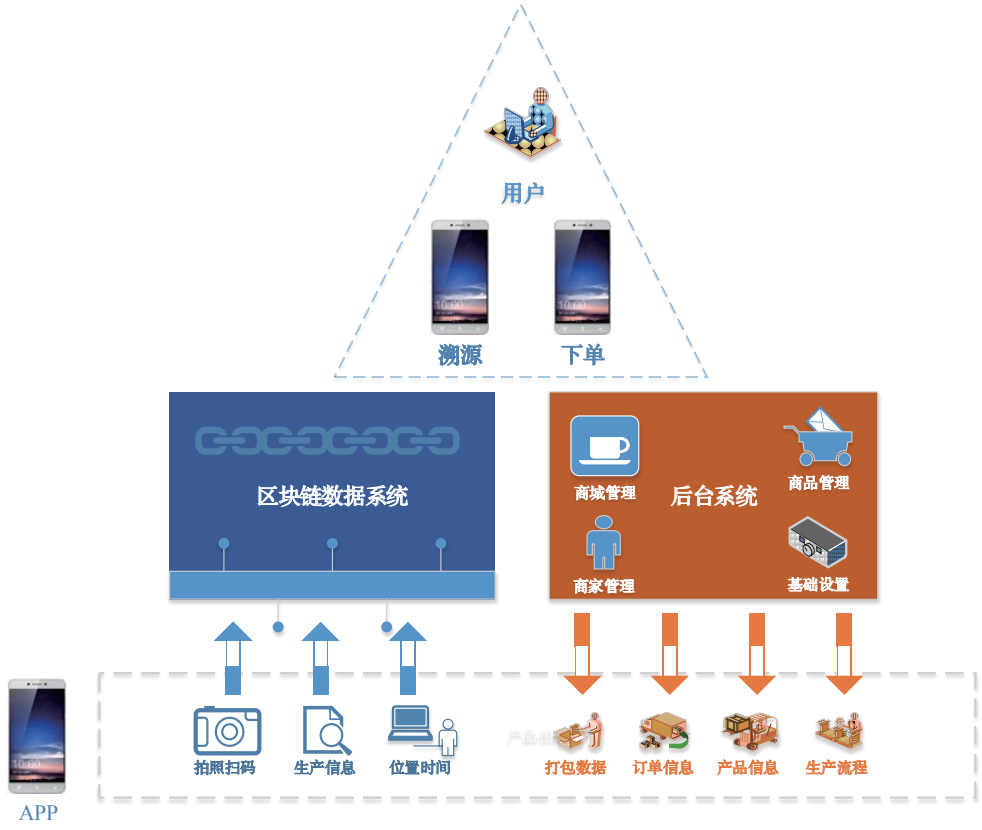

图 7 “哪儿来”区块链系统拓扑结构图

5 结论

区块链溯源系统以每个农产品作为溯源对象，能够对其生产、加工以及采摘后流通环节进行全程的数据记录。通过区块链系统去中心化、不可篡改的特点将数据进行存储，保证数据的可靠性 [25]。此外，本系统具备良好的扩展性和可移植性，数据采集通过客户端 / 服务器架构实现，查询系统与微信等社交平台相融合并结合溯源查询二维码，为消费者提供从“农

田到餐桌”的全过程追溯。系统经实地部署、测试和应用，实现了农产品溯源数据在区块链上的安全、可靠存储以及不被篡改，同时能够有效实现农产品的溯源。

参考文献

[1] 邓勋飞, 吕晓男, 郑素英,等. 基于GIS的农产品安全溯源体系[J]. 农业工程学报, 2008(s2):172-176.

[2] Swan M. Blockchain: Blueprint for a New Economy[M]. California: O'Reilly, 2015.

[3] 郑业鲁, 刘晓珂, 郭洛先,等. 基于供应链的蔬菜安全溯源系统的设计与实现[J]. 广东农业科学, 2016, 43(1):145-150.

[4] Kosba A, Miller A, Shi E, et al. Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts[C]. Security & Privacy. IEEE, 2016:839-858.

[5] De Silva J. Supply chain - Putting theory intopractice[J]. 2009.

[6] 林小驰, 胡叶倩雯. 关于区块链技术的研究综述[J]. 金融市场研究, 2016(2):97-109.

[7] 刘万星. 基于去中心化网络的数据存在性证明系统的设计与实现[D]. 桂林: 桂林理工大学, 2016.

[8] 伍旭川, 王鹏. 区块链技术应用及展望[J]. 清华金融评论, 2016(10):23-25.

[9] 傅俊, 曹春益. 基于物联网的农产品质量溯源系统设计[J]. 软件, 2014(3):9-10.

[10] Zyskind G, Nathan O, Alex. Decentralizing Privacy: Using Blockchain to Protect Personal Data[C]. IEEE Security and Privacy Workshops. IEEE Computer Society, 2015:180-184.

[11] 丁庆洋, 朱建明. 区块链视角下的B2C电商平台产品信息追溯和防伪模型[J]. 中国流通经济, 2017,31(12):41-49.

[12] 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.

[13] 梅臻, 康雅丽. 区块链技术在金融领域的应用与法律思考[J]. 上海金融学院学报, 2017(4):41-50.

[14] Github. Go Ethereum[EB/OL]. [2018-01-11]. https://github.com/ethereum/go-ethereum.

[15] Ethereum Foundation. About the Ethereum Foundation[EB/OL]. [2018-01-11]. https://www.ethereum.org/foundation.

[16] 刘江, 霍如, 李诚成,等. 基于命名数据网络的区块链信息传输机制[J]. 通信学报, 2018(1):24-33.

[17] Donet J A D, Pérez-Solà C, Herrera-Joancomartí J. The Bitcoin P2P Network[C]. The Workshop on Bitcoin Research. 2014:87-102.

[18] 解菁, 孙传恒, 周超,等. 基于GPS的农产品原产地定位与标识系统[J]. 农业机械学报, 2013, 44(3):142-146+152.

[19] The go-ethereum Authors. Official Go implementation of the Ethereum Protocol[EB/OL]. [2018-01-11]. https://geth.ethereum.org.

[20] Iancu B, Sandu C. A Cryptographic Approach for Implementing Semantic Web's Trust Layer[M]. Innovative Security Solutions for Information Technology and Communications. Berlin: Springer International Publishing, 2016.

[21] Wright A, De Filippi P. Decentralized Blockchain Technology and the Rise of Lex Cryptographia[J]. Social Science Electronic Publishing, 2015.

[22] Yang Y. Semantic Information Retrieval over P2P Network[C]. Conférence En Recherche D'infomations Et Applications - Coria 2011, French Information Retrieval Conference, Avignon, France, March 16-18, 2011 . Proceedings. 2011.

[23] Biryukov A, Khovratovich D, Pustogarov I. Deanonymisation of Clients in Bitcoin P2P Network[J]. Eprint Arxiv, 2014:15-29.

[24] 安庆文. 基于区块链的去中心化交易关键技术研究及应用[D]. 上海: 东华大学, 2017.

[25] Alireza B, JooSeok S. Trend of centralization in Bitcoin's distributed network[C]. IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/distributed Computing. IEEE Computer Society, 2015:1-6.