

分数：

--

# 《区块链技术》大作业报告

## 基于区块链的食品安全溯源设计

学 院（系）： 电子信息与电气工程学部

专 业： 计算机科学与技术

班 级： 电计 2001

姓 名： 陆鑫

学 号： 20203015022

指 导 教 师： 王鹏飞

**大连理工大学**

Dalian University of Technology

## 一、概述

近几年，各类食品质量安全事件的出现，使得消费者对于我国的食品安全现状产生了严重的信任危机，人们对于食品安全的重视程度也不断提高，在此背景下，各种溯源技术应运而生。针对食品安全的溯源主要是指能够通过相应标识实现对食品来源的溯源，并提供从开始生产阶段到最终食品端上餐桌全过程各种信息的详细展示。一旦出现食品安全质量问题，通过标识能够溯源并定位问题发生的具体环节，将其相应的责任明确到个人，从而进一步缩小食品安全事件的影响范围。由于当前食品的种类和数量越来越多，使得传统的食品安全溯源技术已经无法适应现状，逐渐出现了食品安全溯源不及时、溯源信息不准确等问题。于是，区块链技术凭借低成本、高效率、分布式等应用优势，在各个领域得到了十分广泛的应用。

## 二、国内外研究现状

### 1) 国外研究现状

国外对于食品安全溯源这一类的研究起步较早，以下是国外在食品安全溯源信息化建设方面这几年的研究成果。

Abid Haleem 等人（2019）认为，食品掺假、欺诈和食源性疾病的大量爆发，动摇了消费者对所消费食品的信心，这些事件迫使食品供应链合作伙伴在其各自的供应链中实施适当的可追溯系统，以维持消费者的信心。他们主要研究了在 FSC 追溯系统成功实施中起重要作用的驱动因素，并评估其中发展的因果关系。过程中，雇用了一些司机来进行试验排名，这些司机排名基于突出和效果评分。结果表明，驾驶员被分为两组：原因组和结果组。4 名驾驶员属于原因组，其余 8 名驾驶员属于结果组。最具影响力的驱动力是“食品安全和质量”，这对可追溯体系的实施产生了重大影响。他们开发的系统能够作为 FSC 内可追溯系统架构开发的基础，并协助政策制定者及实务人员识别及评估与 FSC 内可追溯系统实施相关的驱动因素，也为实践者和管理者在可追溯性实现相关问题上的决策提供了有用的见解和支持。

Dorota Miarka 等人（2019）认为对食品供应链上的所有参与者来说，使“追踪”食品路线成为可能，应该成为一项法律要求。它允许识别和监控整个供应链中原材料、废料和成品的运输和使用。他们在对包装大豆油进行 BRCv7（英国零售协会，第 7 期）审计期间，对可追溯系统进行了案例研究。他们的分析基于 SOP（标准操作程序）、HACCP（危害分析和关键控制点）程序和记录，包括关于关键控制点的程序和记录，以及来自内部软件制造 WHM（WebHost Manager）（查询版本 5.2.8）的数据。他们追踪记录了原材料、添加剂以及成品和客户的批次，通过这些实验验证，发现在系统中存在不符合实际的情况，需要将其加入纠正清单。它们的修正是满足标准要求和系统改进的先决条件的。纠正措施包括对生产可追溯性的操作程序和相关文件进行补充，并记录原材料和包装的监督 and 验证。为了减少包装油过程中产生的损失，对机器和电器的控制程序进行了修改。针对程序中引入的变化对员工进行了培训，并确认了这些措施的有效性，证明了采取纠正措施的必要性。

### 2) 国内研究现状

食品安全现阶段涉及到生活中的方方面面，其中就含有消费者的生命身体安全、身体健康有序、经济平稳发展、社会安定和谐及国家政府的形象。根据国务院之前发布的相关食品安全的工作安排，希望各地区积极响应搭建“统一、规范的食品质量安全标准体系”、“食品质量安全例行监测制度”、“食品质量安全追溯制度”。由此可见，食品安全问题已经成为全社会的关注焦点。在生活中，为了有效避免消费者食用有害食品、传播食品中携带的有害传染病菌，保障食品安全，建立一个可以快速跟踪以及及时报警的系统迫在眉睫。

我国对于食品安全问题十分的重视，近年来一直致力于开展食品安全溯源系统的研发，也取得了一定的研究成果。

在对食品安全溯源的研究中，通过对相关文献进行研究分析发现，近年来学者对食品安全溯源体系的研究方法不断增多，且研究程度不断加深。本文整理了2014年1月至2022年10月中国知网中有关食品安全溯源体系建设方法的文章，如图1所示。图1表明该问题的研究已越来越受到重视。

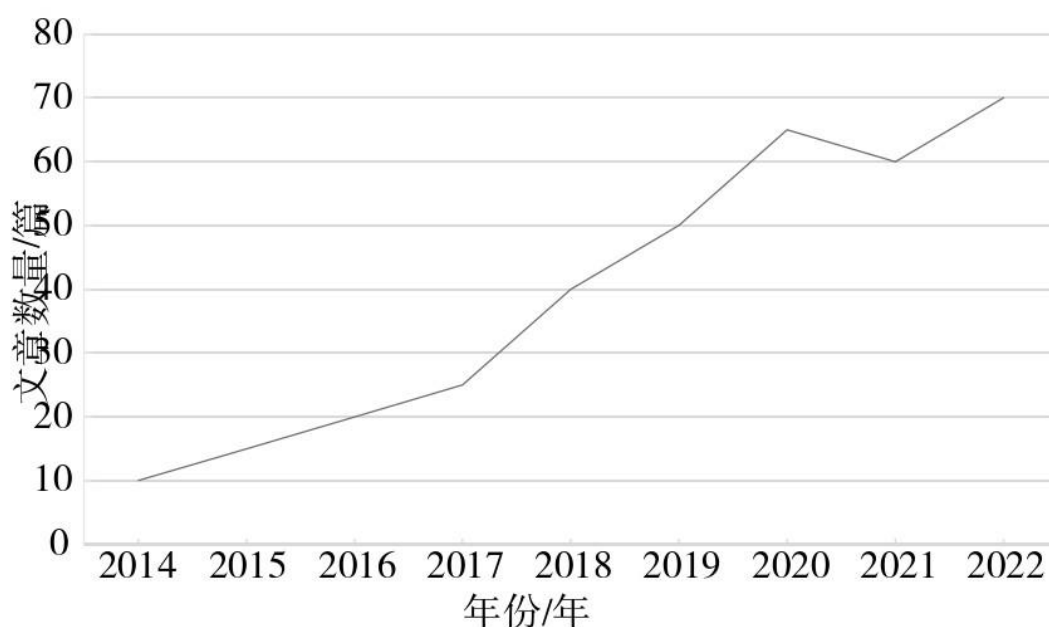


图 1 2014 年 1 月至 2022 年 10 月知网关于食品安全溯源体系研究的文章数量

姚新华采用射频识别技术（Radio Frequency Identification,RFID）与网络技术结合，实现了所有环节的食品安全信息可查，食品溯源管理系统利用 RFID 技术，从食材源头到食品生产加工、运输和流通做到全环节可溯源。但 RFID 应用于校园食品安全溯源中存在很多缺点，RFID 技术不够成熟且 RFID 电子标签相对于普通条码标签价格较高，此外 RFID 技术在安全上也存在很大的隐患，由于 RFID 电子标签信息可能会被非法读取或恶意篡改，无法完全保证食材的来源可靠，因此采用 RFID 射频技术方法溯源校园食品来源并不可靠。鉴于区块链技术的安全性，徐睿等对区块链技术溯源食品安全问题进行了深入研究，指出区块链用于溯源系统的建设，国外发展势头迅猛，很多国外企业已将区块链溯源系统用于商用，在农业流通环节引入区块链技术确保信息透明。

### 三、区块链设计

#### 1) 体系层次及其实现

溯源系统的技术架构如图 2 所示，主要分为物理层、通信层、数据库层和接口层。其中区块链技术用于数据库层和通信层。

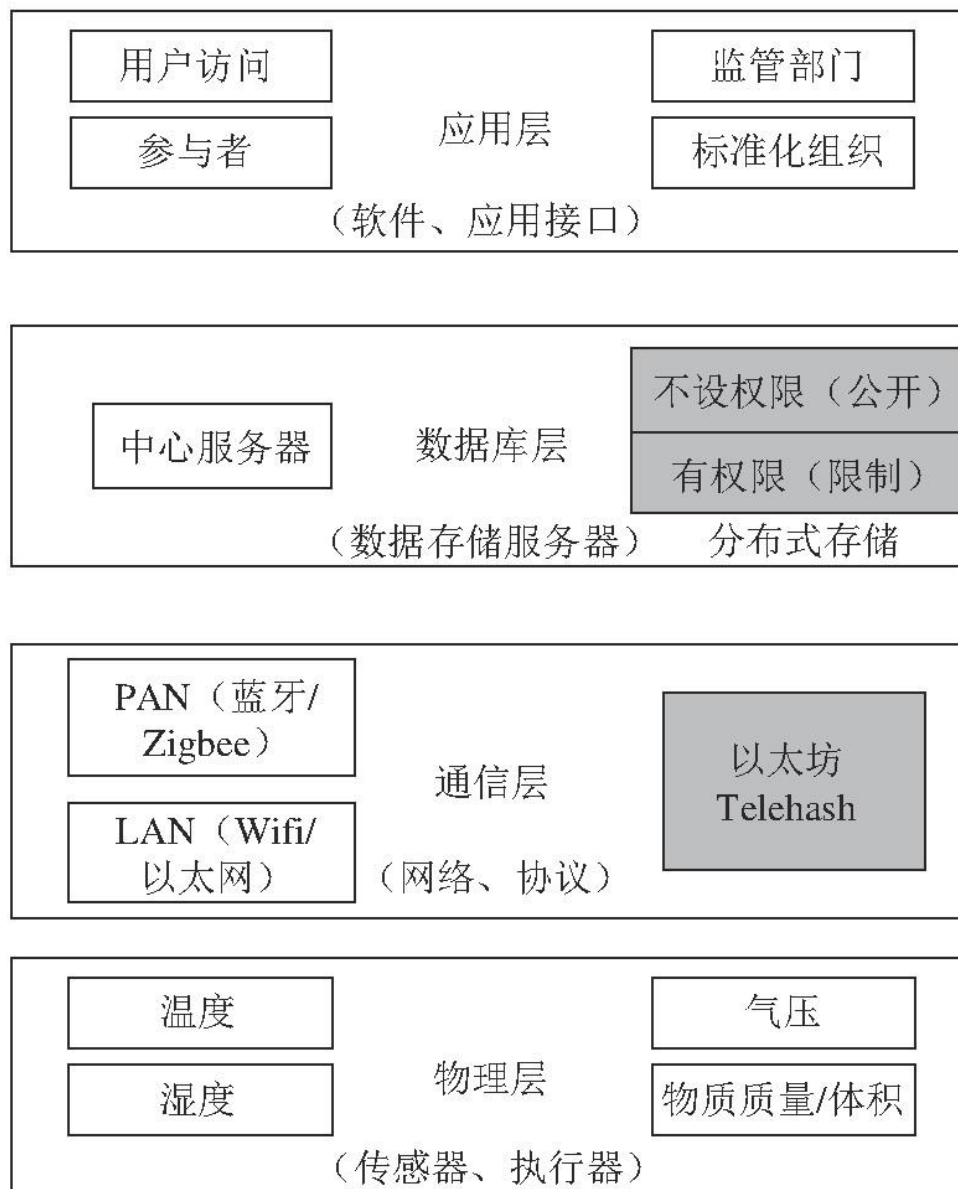


图 2 溯源系统的技术架构

物理层中主要包含了智能传感器与执行器等，用于数据采集并转发到上层协议，实质上与物联网结构中的物理层相似。设备采用的密码加密技术和访问控制机制使其易受攻击，供应商可从路由器、通信协议等方面对其安全性进行加强。

通信层主要包括网络结构与协议。传统物联网架构的通信层主要采用蓝牙、Zigbee、Wifi、以太网、3G/4G 等通信机制。溯源系统的通信层应用基于区块链技术的以太坊平台、Telehash 信息传递协议，以防止被攻击节点通过网络破坏系统。

数据库层主要指分布式存储数据库。区块链中每条记录都包含时间戳及唯一的加密

签名,同时完整的交易记录可供任何合法用户进行验证与审核。公有链中不设访问权限,信息记录对网络中所有节点公开,优点在于账本便于审查且具有高透明度,不足之处是执行共识机制的时间成本与耗能较大。在联盟链和私有链中,可访问到账本的合法用户仅是被授权的指定节点。故为增强系统可扩展性与执行效率,联盟链是更佳选择。

接口层(或应用层)主要嵌入应用程序或协议,提供人机交互入口。

在产品从生产到消费的全过程中,涉及到的参与者角色及其职责如下:注册机构:为其他参与节点提供唯一的身份账号;标准化组织:定义标准条例并有修改权利;原材料供应商、生产企业、加工制造企业、分销商、零售商:向区块链输入指定产品的主要信息;消费者:购买食品产品,有访问产品特定信息的权限。本文所提出的基于区块链的食品溯源网络架构如图3所示。

从参与者角度来看,首先所有参与者在注册时会创建一个对应的信息档案,档案内应对其企业信息、职能、地址、资格认证等必要信息进行记录。参与者在成功注册后,将会获得一个公钥和私钥,公钥向区块链中全体成员公开,而私钥作为交易过程中验证身份与信息的关键。每个参与者都可以利用已注册ID登录用户界面,进入指定区块链网络。该软件的开发与维护工作须由可信任的单位来负责,并要有权威的组织机构来承担注册机构的职责。

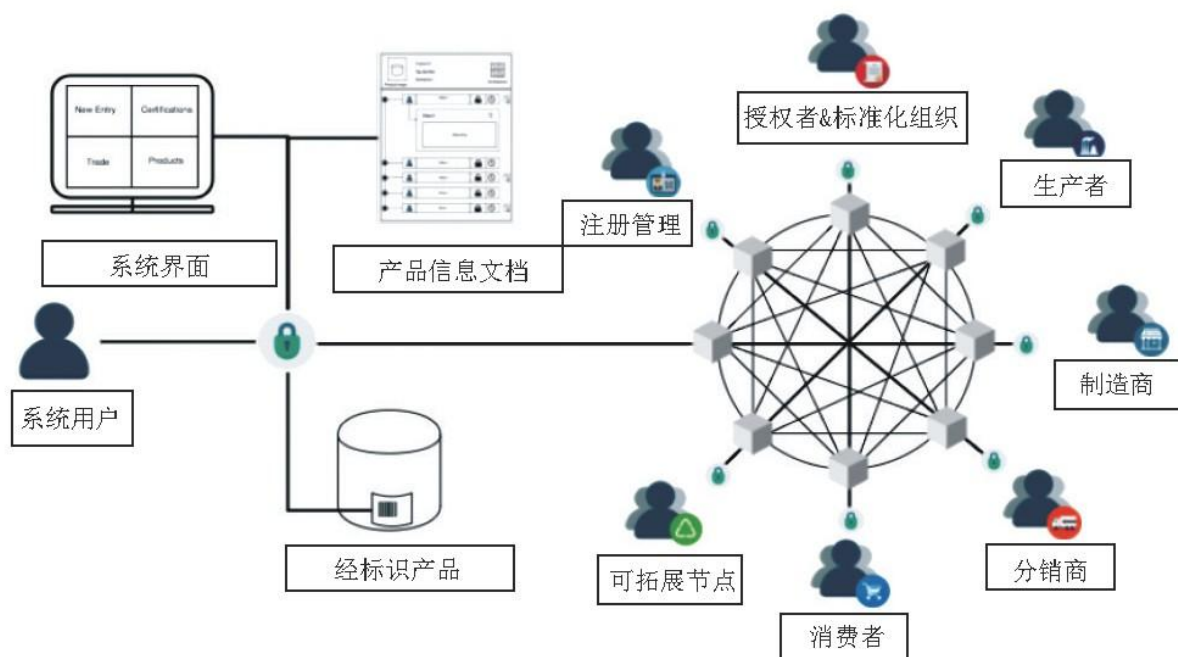


图3 区块链中的食品溯源网络架构图

从信息流来看,所有信息都存储在区块链中并且支持被授权的节点对其进行访问。信息存取的权限又取决于参与者在供应链中的角色与职能。此外,区块链的运行规则由代码定义并存储在区块链中,无法被区块链中的某一参与者所修改,从而保证数据的真实性与有效性。若要改变区块链运行规则,则同数据存储一样,需要向全部节点进行广播并且由重点部门核实确认。

显然,食品溯源链条中会涉及权限角色地位不等的各机关和企业,由此重申选用联盟链的意义。联盟链与公有链的区别不仅在于系统中心化与参与者身份,还有共识机制与激励机制上的差异。选用联盟链意味着:1) 区块链系统中的信任机制不再要求是 PoW 或 PoS,可以通过降低去中心化程度的方法减少参与共识机制的节点以克服挖矿过程的

资源浪费问题。2) 维护食品溯源系统是联盟链中各参与节点的责任，故区块链系统的运行无需激励机制，即选用联盟链，可以不依赖数字货币，简化记录账簿，降低系统运行所需带宽。

## 2) 运行机制分析

在设想的溯源系统中，每一样商品都在区块链网络中被数字化，包括其身份标识及参数信息，信息维护者方可全面具体地维护产品信息，避免溯源信息割裂问题。利用产品和参与者的标识，认证授权中心可以通过智能合约的方式自动对产品当前担责节点开放权限，保证数据维护的有序性与可靠性，防止非相关节点违规操作，实现系统有序、严谨、全面地跟踪产品并维护产品信息。

在被授权参与者维护产品信息文档时，要求必须以私钥连接到网络后，在软件应用界面进行数据信息输入。系统要收集一系列信息，包括产品当前状态、产品类型、所依据的行业标准等。一旦参与者发起产品转移，系统通过内嵌的智能合约，对数据格式是否合法及是否符合行业标准等方面进行审核，验证成功后，将该参与者之前提供的信息打包录入。由此可见，数据打包成区块的时间节点是可控的，从而保证内部溯源数据不会与外部溯源数据被封装进同一区块，造成区块信息访问权限发生矛盾（为保护企业隐私，内部溯源信息的访问权限必然高于外部溯源信息）。被授权的节点在与另一节点进行“交易”时，比如当产品从加工厂流动到物流企业时，产品所属关系被转移，两节点之间需要达成统一协议并数字签字。数字签名利用了非对称加密技术，保证了信息不被篡改且两节点的身份信息无需公开。当“交易”在区块链网络中被核心层节点公证并进行全网广播后，包含交易详细信息的区块按照时间戳顺序成为区块链上的最新环节。一旦交接工作完成，智能合约执行协议内容，系统授权对象将自动从加工厂转移到物流企业，物流企业方可继续维护并补充产品信息。在“交易”过程中，双方对交易信息的加密解密过程通过不对称密钥完成，保证了信息无法被恶意篡改，解决了交易过程中的诚信问题。数据输入简化示意图如图 4 所示。

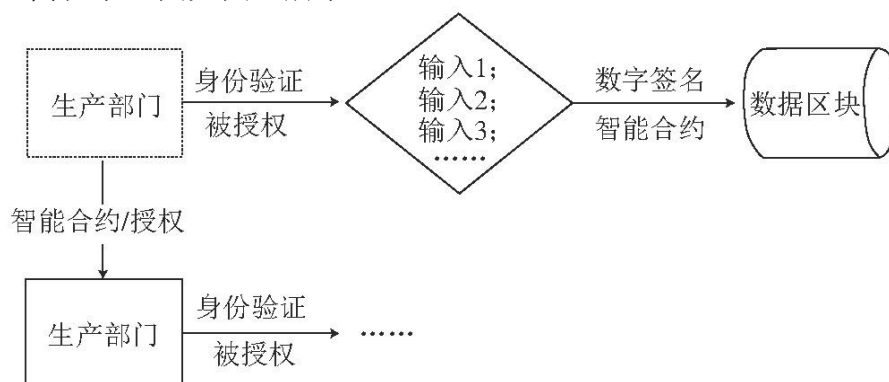


图 4 数据输入过程

综上，企业内部信息维护与企业间交易过程都可以通过区块链来记载操作日志，时间戳技术与不对称加密技术保证了基于区块链技术的食品溯源系统的可靠性和防篡改性。在溯源过程中依赖的产品信息文档中应包含以下几个方面：

产品担责方资料：被授权参与者的资料列表应按照时间顺序记载到当前最新担责方为止。每次产品转移，即被授权参与者发生改变时，系统将会记录关于新的产品担责方的详细信息并添加到产品信息文档中。利用参与者在注册时生成的数字化标签，系统可以便利地进行指定和授权正确的产品担责方。当然，产品担责方信息设有访问限制，避

免造成企业隐私泄露问题。

**时间戳:**当产品信息文档中产生新的输入记录时,系统会自动记录下信息输入的时间点。通过时间戳技术,供应链网络的输入条目满足时间排序,也对防篡改提供了保障。

**位置信息:**为了解产品的物流路线,当有参与者对产品信息进行录入时,系统会根据参与者的位置信息记录产品相应的地理位置。通常,可以利用唯一的 ID 来表示位置信息,有条件的系统也可以通过动态 GPS 数据来提供准确的位置信息。

**产品指定信息:**这部分是食品溯源线索关键所在,同时也是消费者角色最为关注的信息。要求的信息应该能够展示出产品形成过程的投入,甚至为生产、加工、质检部门提供反馈信息。

在溯源系统中,对任何参与者而言,产品信息的体现方式都是产品信息电子文档。产品信息文档模板如下图 5 所示。

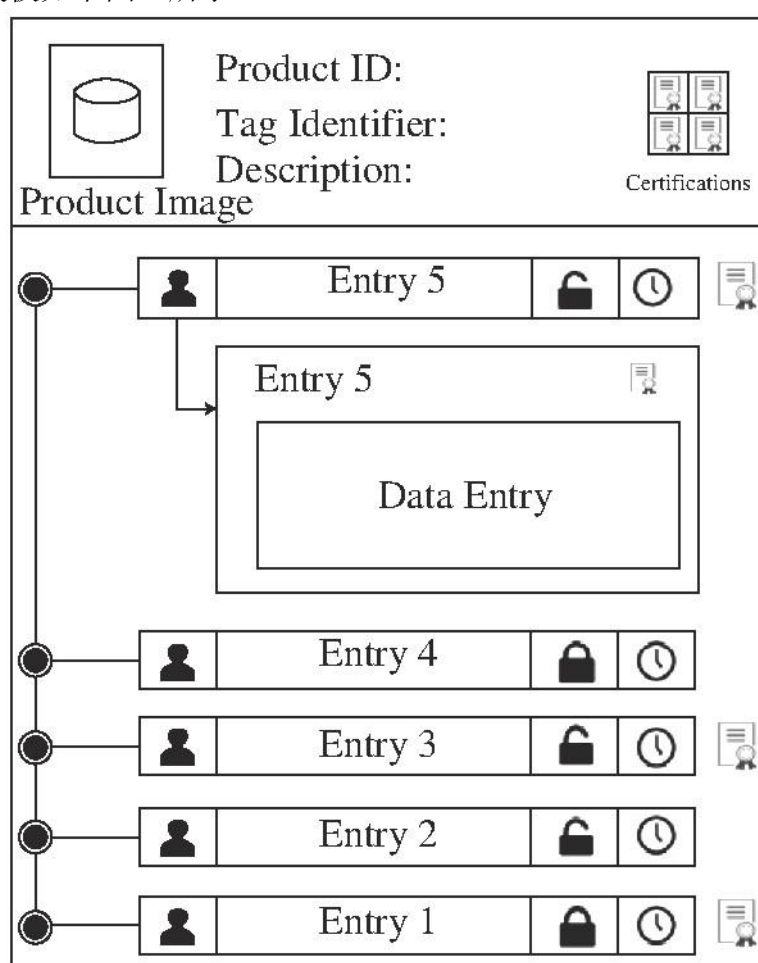


图 5 产品信息文档模板

其中,每条信息输入条目都有时间戳并且由所负责的参与方签名,与产品相关的认证机构信息也包含在内。此外,为了控制用户对信息文档(包括指定的产品信息、参与者的详细信息等)的访问权限,会在产品文档中嵌入一定的规则代码。在参与者访问信息文档时,需要输入其密钥,系统根据其拥有的权限来展示可见内容。

以农产品为例,通过以上食品溯源系统的信息采集,指定蔬菜产品有一个电子信息文档,文档中应当包含了指定信息如产品的收获日期、物流路线与转运的时间节点和其种植地等。购买产品的用户有权利读取以上关键信息,但实际上,信息文档中还包括更



加具体的信息，包括产品生产的农场或基地、产品的生长环境如温度湿度等。这些与顾客无直接关系且涉及到企业隐私的信息只能由区块链中被授权的参与者访问，一般会在发生食品安全问题后访问此类信息。

### 3) 溯源系统应用场景

上文已提出一个基于区块链的食品安全溯源体系，并对其运行机制进行了简要介绍。下文将从实际案例出发，详细描述溯源系统的工作过程。

不妨以农产品溯源为例。农产品追溯系统涉及到农产品的方方面面，包括采生产、保存、运输、销售、售后等整个产品线，这里的每个方面都会有食品安全隐患，因此需要详尽的信息记录。在溯源系统中的溯源是双向的，需要对产品进行回溯和追踪，即来源和去向双向的信息。消费者可以通过扫描产品对应的唯一认证码获取产品的生产场地、保质期等准确信息，以保证买的安心，吃的放心；管理者也可以通过大数据分析出产品贩售去向，归纳得出适宜的销售途径[28]。当然，如果出现了食品安全问题，监管部门也可以通过产品编码快速查到生产厂商，对事情责任人予以法律严惩，做到及时、准确、公正、公开。

正向追踪指的是产品从生产地产出，到经销商售出、消费者购入的整个流程。如果这个流程出现了问题。生产企业可以根据产品编码快速定位生产场地，生产单位。从追溯系统处获得产品流通链，追回有问题产品，降低食品安全风险，增强人民对企业的信心。

反向追溯指的是产品从消费者倒回到生产地的整个过程。消费者可以通过产品唯一编码获取详细信息，向监察部门举报问题产品，在指定的网页页面或是电话沟通产品具体信息。相关部门就可以据此对生产厂商进行追责，依法要求厂商对消费者进行赔偿，并归纳总结问题出现原因以及补救办法，及时整改，防止问题再次发生。

## 四、总结报告

基于区块链技术的食品安全溯源研究从根本上来讲是一项需要不断改造且创新的技术研究工作，不过就目前已有的精力与业务知识的匮乏，本文仅仅只针对基于区块链技术的蔬菜物流信息源等一系列的溯源考量模式进行了综合分析以及系统的整体设计，从长远来看，对目前创建食品安全溯源系统还是需要更进一步的具体研究。本文根据区块链的工作原理及技术特征，设计了基于区块链的食品溯源体系设计，并从实际应用场景出发验证设计方案的可行性与有效性。目前基于区块链的食品溯源案例鲜少，大多应用于企业内部溯源过程，仅仅发挥了区块链作为分布式存储数据库的特性。同时创新性地提出了基于区块链的食品溯源体系方案，从溯源体系顶层架构出发，描述出区块链在溯源体系中的技术落脚点，并在区块链的去中心化程度、共识机制等方面加以改进以克服原始区块链（公有链）的缺点，使区块链系统在食品溯源体系中的应用在发挥优势的同时，不给宿主系统带来负担。

通过此次区块链技术大作业，我掌握了区块链的基本原理及其在食品安全溯源领域的应用，加深了课堂上学习的理论知识。通过查阅文献资料，我了解到传统的食品安全溯源问题的长期痛点，如可追溯，不可篡改，去中心化，而这些问题都可以通过区块链技术得到很好的解决。总之，此次大作业让我学到了许多未曾接触过的知识，受益匪浅。