分类号： 密 级：公开

学 号：20202008001 单位代码：10759

石河子大学

硕 士 学 位 论 文



基于区块链的农产品溯源关键技术研究

学 位 申 请 人 刘陕南 指 导 教 师 刘长征 教授 申请学位门类级别 工学硕士 学科、专业名称 农业工程

研 所

究 在

方 学

向 农业信息化技术及应用 院 信息科学与技术学院

中国 ·新疆 ·石河子 2023 年 6 月

**Blockchain-based Key Technology Research on Agricultural Product Traceability**

A Dissertation Submitted to

**Shihezi University**

In Partial Fulfillment of the Requirements for the Degree of

**Master of Engineering By**

**Liu Shan-nan**

**(Agricultural Engineering)**

Dissertation Supervisor: Prof. Liu Chang-zheng

摘要

近年来，农产品安全问题在学术界和商业界引起了极大的关注。一系列农产品安全事故接连发 生，例如镉大米、硫磺姜以及毒豆芽等，它们严重的破坏了消费者对农产品行业的信心，不仅会影 响经济的正常发展，还会危及社会的稳定。实现对农产品生产和流通信息的监管和追溯，是减少农 产品安全事故的有效举措。现有的农产品溯源系统模式单一，数据存储在中心化的数据库中，数据 不透明，商家因自身利益可以任意修改农产品质量数据，同时，缺乏监管部门参与，农产品质量的 可信度低。区块链技术能够有效的解决这些问题， 区块链技术的去中心化、分布式存储、公开透明、 不可篡改等优点，更紧密地联系农产品供应链的参与者和监管者，有效解决集中追溯方式存在的问 题，提高农业食品的安全性和质量，改变农业产业的许多方面。本文针对现有农产品溯源的弊端， 提出基于区块链的农产品溯源关键技术研究，主要研究内容如下：

1）设计了基于区块链的溯源方案及模型。针对现有的农产品追溯系统存在数据不可见、敏感信 息泄露等问题，设计了一个基于联盟链和智能合约的农产品供应链追踪方案和模型，结合农产品供 应链的全过程，定制化设计了数据管理模式和智能合约，以确保农产品生产和流通信息的公开透明。

2）提出了改进的实用拜占庭容错算法 T-PBFT(Traceability-Practical Byzantine Fault Tolerance) 。 改进的针对目前农产品溯源与区块链技术相结合的应用中存在的时延高、系统开销大、支持的规模 小等问题，提出了一个基于分组和信用投票的改进实用拜占庭容错算法 T-PBFT。该算法结合农产品 供应链的特点，优化了原算法中的一致性协议，通过响应速度将大规模网络节点划分为不同的分组， 进行分组共识；提出了信用模型与投票机制，根据节点在共识中的行为动态更新节点状态，评估节 点的可靠性，同时作为选举管理节点的依据。实验结果表明，改进的 PBFT 共识算法为农产品溯源 系统提供了更小的延迟、更高的吞吐量，可以支持更大规模的追溯，有效地改善网络节点间通信量 急剧增加的问题，减少恶意节点的影响。

3）将上述设计的溯源方案、模型以及改进的共识算法应用在区块链系统中。以有机大米的销售 为背景，分析了系统需求、系统功能等， 进行概要设计，最后使用超级账本框架实现有机大米溯源， 并对系统性能进行测试，以确保其实用性。结果表明，农产品供应链追溯系统能够实现从“农场到 餐桌”的信息可追溯和可共享，打破企业之间的信息孤岛，消除对中央机构的依赖，提高交易记录 的完整性、可靠性和安全性，能够重建公众对农产品安全的信心。

关键词：区块链；农产品溯源；共识机制；PBFT；有机大米

**Abstract**

In recent years, the safety of agricultural products has become a major concern in both academic and commercial sectors due to a series of incidents such as cadmium rice, sulphur ginger, and tainted bean sprouts. These incidents have seriously undermined consumers' confidence in the agricultural industry, affecting not only the normal development of the economy but also endangering the stability of society. Achieving the supervision and traceability of information on the production and circulation of agricultural products is an effective measure to reduce agricultural safety incidents. However, the existing agricultural product traceability system has a single model with data stored in a centralized database, lacking transparency. Businesses can arbitrarily modify agricultural product quality data for their own interests, and regulatory authorities lack participation, resulting in low credibility of agricultural product quality. Blockchain technology can effectively solve these problems. The advantages of blockchain technology, such as decentralization, distributed storage, openness and transparency, and non-tamperability, can link participants and regulators in the agricultural product supply chain more closely. This can effectively solve the problems of the centralized traceability method, improving the safety and quality of agricultural food and changing many aspects of the agricultural industry. This thesis proposes key technology research of agricultural products traceability based on blockchain, taking into account the drawbacks of the existing agricultural product traceability system. The main research contents are as follows.

1) A blockchain-based traceability scheme and model has been developed to address the issues of data invisibility and sensitive information leakage in existing agricultural traceability systems. The scheme and model utilize consortium chains and smart contracts, and cover the entire process of the agricultural supply chain. The data management model and smart contracts have been customized to ensure transparency and openness of agricultural production and circulation information.

2) An improved practical Byzantine fault tolerance algorithm T-PBFT (Traceability-Practical Byzantine Fault Tolerance) is proposed. To address the problems of high time delay, high system overhead, and limited support scale in the current application of combining agricultural products traceability with blockchain technology, an improved practical Byzantine fault tolerance algorithm, T-PBFT (Traceability-Practical Byzantine Fault Tolerance), has been proposed. The algorithm takes into account the characteristics of the agricultural supply chain, optimizes the consistency protocol in the original algorithm, divides large-scale network nodes into different groups by response speed, and performs group consensus. It also proposes a credit model and voting mechanism, dynamically updates the node status according to the nodes' behavior in consensus, evaluates the reliability of nodes, and serves as a basis for electing management nodes. Experimental results show that the improved PBFT consensus algorithm provides smaller latency and higher throughput for the agricultural traceability system, supports larger-scale traceability, effectively mitigates the communication problem between network nodes, and reduces the influence of malicious nodes.

3) The traceability scheme, model, and improved consensus algorithm have been applied to the blockchain system, with the sale of organic rice serving as a case study. The system requirements and functions were analyzed, an outline design was carried out, and the organic rice traceability was implemented using the super ledger framework. The system performance was tested to ensure its practicality. The results indicate that an agricultural supply chain traceability system can achieve traceability and shareable information from farm to fork, break down information silos between enterprises, eliminate reliance on central organizations, improve the integrity, reliability, and security of transaction records, and rebuild public confidence in the safety of agricultural products.

**Key words:** blockchain; agricultural traceability; consensus mechanism; PBFT; organic rice

目 录

[第 1 章 绪论 1](#bookmark2)

[1.1 研究背景及意义 1](#bookmark3)

[1.1.1 研究背景 1](#bookmark4)

[1.1.2 研究意义 2](#bookmark5)

[1.2 国内外发展现状 2](#bookmark6)

[1.2.1 传统农产品溯源研究现状 2](#bookmark7)

[1.2.2 基于区块链的农产品溯源研究现状 3](#bookmark8)

[1.2.3 国内外研究现状总结 5](#bookmark9)

[1.3 研究内容和技术路线 5](#bookmark10)

[1.3.1 研究内容 5](#bookmark11)

[1.3.2 技术路线 6](#bookmark12)

[1.4 论文组织结构 7](#bookmark13)

[第 2 章 区块链相关理论与关键技术 8](#bookmark14)

[2.1 区块链技术 8](#bookmark15)

[2.1.1 区块链概念 8](#bookmark16)

[2.1.2 区块链分类 8](#bookmark17)

[2.2 智能合约 9](#bookmark18)

[2.3 共识算法 10](#bookmark19)

[2.4 超级账本 Hyperledger Fabric 11](#bookmark20)

[2.5 IPFS 技术 11](#bookmark21)

[2.6 本章小结 12](#bookmark22)

[第 3 章 基于区块链的溯源方案设计及模型构建 13](#bookmark23)

[3.1 传统农产品溯源方案分析 13](#bookmark24)

[3.2 基于区块链的溯源流程分析 13](#bookmark25)

[3.3 基于区块链的溯源方案设计 15](#bookmark26)

[3.3.1 区块链平台选择 15](#bookmark27)

[3.3.2 智能合约设计 16](#bookmark28)

[3.3.3 数据存储设计 18](#bookmark29)

[3.4 基于区块链的溯源模型构建 20](#bookmark30)

[3.5 本章小结 21](#bookmark31)

[第 4 章 基于农产品溯源的 PBFT 算法优化 22](#bookmark32)

[4.1 PBFT 共识算法 22](#bookmark33)

[4.1.1 PBFT 算法的一致性协议 22](#bookmark34)

[4.1.2 PBFT 算法的视图切换协议 24](#bookmark35)

[4.1.3 PBFT 算法的检查点协议 24](#bookmark36)

[4.1.4 PBFT 算法存在的缺陷 24](#bookmark37)

[4.2 T-PBFT 算法设计 24](#bookmark38)

[4.2.1 T-PBFT 算法整体思路 25](#bookmark39)

[4.2.2 分组策略 25](#bookmark40)

[4.2.3 信用模型与投票机制 27](#bookmark41)

[4.2.4 T-PBFT 算法流程 28](#bookmark42)

[4.3 实验验证 30](#bookmark43)

[4.3.1 T-PBFT 算法吞吐量测试 30](#bookmark44)

[4.3.2 T-PBFT 算法共识延迟测试 32](#bookmark45)

[4.3.3 T-PBFT 算法通信次数测试 33](#bookmark46)

[4.3.4 T-PBFT 算法安全测试 34](#bookmark47)

[4.4 本章小结 36](#bookmark48)

[第 5 章 农产品溯源系统的应用实现 38](#bookmark49)

[5.1 系统角色需求分析 38](#bookmark50)

[5.2 系统功能分析 39](#bookmark51)

[5.3 系统业务流程设计 40](#bookmark52)

[5.4 系统架构设计 42](#bookmark53)

[5.5 系统功能实现 43](#bookmark54)

[5.5.1 环境配置 43](#bookmark55)

[5.5.2 系统功能展示 43](#bookmark56)

[5.6 本章小结 46](#bookmark57)

[第 6 章 结论与展望 47](#bookmark58)

[6.1 结论 47](#bookmark59)

[6.2 展望 47](#bookmark60)

[参考文献 49](#bookmark61)

第 1 章 绪论

1.1 研究背景及意义

1.1.1 研究背景

农产品作为一种食品来源，其质量和安全与人类健康密切相关。近年来， 随着农业 技术的发展，农产品的生产和加工逐渐智能化，但其质量和安全问题越来越严重[1]。水 果、蔬菜等农产品的质量、安全事故频繁发生， 成为人们关注的焦点。为此， 相关研究 者开发了农产品可追溯性系统[2] ，使农产品生产过程透明，并在一定程度上实现了农产 品信息的可追溯性。然而， 农产品的供应链十分复杂，使得农业安全监督和可追溯性在 实践中极具挑战性。因为它包含了多种参与者， 例如农户、加工厂、零售商、运输商等， 同时，农产品供应链包含了大量的数据。而且目前大多数可追溯系统都由第三方管理和 维护，属于集中式体系结构，如企业或政府机构，这就导致了诸如不安全的数据存储， 低可追溯性，单点攻击漏洞和数据隐私等[3] 。可信可追溯是指能够保证可追溯信息的安 全性、完整性、可用性和透明性， 解决集中、垄断、不对称等信任问题。如何实现农产 品的可信可追溯越来越引起了学术界和商业界的关注[4]。实现上述目标的一个潜在解决 方案是区块链技术，区块链技术日益成熟，可以精确地解决目前农产品可追溯系统中存 在的问题，确保数据的完整性，防止篡改和单点故障。

通常，区块链可以被认为是一个分布式数据库，被称为分类帐，它利用一种加密算 法来创建一个按时间顺序排列的由数据块组成的链结构，在点对点网络中发生的所有交 易的记录都可以存储在块中[5]。区块链还集成了多种技术，如点对点（Peer-to-Peer, P2P） 网络、共识机制、加密技术、智能合约等[6]。利用区块链技术对农产品进行追踪， 可以解 决现有追踪系统中存在的问题。区块链主要分为三类： 公有链、联盟链和私有链[7]。联盟 链是指多个组织共同参与和管理的区块链。在隐私方面， 联盟链介于公有链和私有链之 间，数据只能由联盟的成员访问，联盟链的交易效率也高于公有链[8]。在追溯系统中， 农 产品供应链的主要责任方与供应链参与者之间为合作关系，机构间不能完全信任，因此， 本文选择了联盟链作为基本网络。

然而，即使区块链技术可以确保可追溯数据的安全存储和信息源的追踪，使农产品 具有可信赖和可追溯性，直接在区块链上处理和存储农产品可追溯信息仍然面临着新的

挑战[9]，例如交易处理能力差、系统开销大、支持的规模小等。因此， 如何将区块链与农 产品追溯更好的融合，以确保农产品数据来源的安全性、可追溯性、不变性和可达性是 本文的研究重点。

1.1.2 研究意义

通过农产品追溯，可以迅速确定农产品的生产来源和分销渠道，并可以了解食源性 疾病暴发的原因，帮助我们确定污染发生的地点和环节。此外， 高质量、准确的可追溯 信息还可以证明农产品配送过程中是否严格遵守了相关要求，并直接证明了农产品的健 康性。此外， 农产品信息可以验证农产品的真实性，相关的质量参数可以证明农产品价 格的合理性，同时也可以降低农产品欺诈问题的发生。在出现农产品安全和质量问题时， 可以快速识别有问题的农产品，定位问题的关键环节，确定问题的责任主体，及时召回 有问题的产品，并最大限度地减少的损失，为解决农产品安全问题提供了有效的途径。

1.2 国内外发展现状

1.2.1 传统农产品溯源研究现状

为了应对日益增长的农产品安全问题，人们开发了很多溯源系统，条形码是其中之 一。最初， 条形码以宽度（线）和平行线的间距表示数据，可以称为线性或一维条形码 或符号系统。每个国家都有自己的识别代码， 数据存储在这些行之间。由于它是一个一 维系统，因此与作为二维数据捕获机制的快速响应数据矩阵相比，它存储的数据更少。 目前，使用条形码基本上是为了商品的定价，而不是为了跟踪产品。快速响应（Quick Response, QR）码是作为二维条形码引入食品行业的另一个可追溯系统。二维码可以嵌 入文字、视频、广告、个人信息等， 可以集成到用户智能手机应用程序中，可以通过扫 描二维码，查看提供的有关产品的信息[10] 。一维码通常携带不超过 100 字节的信息，二 维码可以携带更多的信息，并具有一定的错误检测和纠错能力，如 PDF417 码可以携带 1108 个 ASCII 字符。还有一些公司依赖物联网（Internet of Things, IoT）应用程序来改 进农产品供应链的可追溯性过程。RFID（Radio Frequency Identification）、传感器和无 线技术为整个农产品供应链提供了可追溯性和监控解决方案，也使自动供应链跟踪的操 作成本几乎为零。RFID 标签可以存储 16k-64k 字节，与二维码相比，大大增加了存储容 量。物联网系统可以从各种设备中读取数据， 包括智能标签（RFID、NFC、条形码、蓝 牙、激光扫描仪和其他信息传感设备和智能嵌入式技术） ，以及环境温度和湿度、车速

和地理定位等感官数据。物联网为供应链的可追溯性带来了许多好处， 包括温度调节和 更准确的跟踪、更好的质量控制、安全、供应链过程优化和降低成本， 特别是在产品召 回的情况下。文献[11]提出了一个系统是基于 RFID 的半自动可追溯性平台，旨在通过自 动化来测试和评估可追溯性的有效性。具体来说，系统使用 RFID 标签来读取产品的属 性，通过 RFID 从标签中获取数据，为人员提供个人数字助理设备以及中心化的计算系 统。这个案例的研究显示，RFID 技术在农业可追溯性上的应用可以提供许多优势和改 进，例如更短的数据管理和分析时间。另一种基于中心化的计算系统的可追溯系统是由 文献[12]提出的，该框架的每个产品都带有包括可追溯性代码的印刷标签、有关可追溯资 源的所有必需数据的 XML（可扩展标记语言）文件、以及一个中央数据库，其中存储所 有数据并可供利益相关者使用。当涉及到有限的数据时，该系统既高效又精确。但是， 随着数据量的增加，数据库负载过重，因此需要额外的计算能力。文献[13]对 RFID 和农 业食品供应链可追溯性进行了综述，详细阐述了 RFID 技术在食品供应链中应用的优势 和可能的挑战。此外，还制定了基于云的农业可追溯系统的概念。文献[14]提出了几种用 于环境监测的智能农业技术（如，RGB 相机，激光雷达传感器，热成像相机，土壤湿度 传感器等），这些技术能够收集有关食品质量的信息。采用基于传感器的监控系统可以 限制供应链运营商的手动数据输入，减少工作量并提高前向和后向可追溯性的效率。在 这种情况下，各种网络和设备被连接起来，形成了一个全球网络空间，该网络空间又通 过各种网络物理接口（如传感器）连接到自然空间，形成全球网络物理系统[15]。文献[16]提 出了一种基于物联网、RFID、传感和云技术的监控系统， 能够在有危害分析及关键控制 点（Hazard Analysis and Critical Control Point, HACCP）规范的情况下确保食品质量和安 全。文献[17]提出了一种食品可追溯性监测框架，该框架利用传感技术，能够监测种植环 境，从而深入了解食品的真实性。上述研究工作代表了自动化电子可追溯系统（包括基 于 DLT 的系统）的第一步。这些系统通过使用 RFID、无线传感器网络等通信技术， 提 供或改进了收集农产品可追溯性信息的手段。

1.2.2 基于区块链的农产品溯源研究现状

区块链相关的农产品供应链可追溯性研究在过去几年中受到了广泛的关注，区块链 可能是目前在供应链网络中提供可追溯性相关服务的最有前途的技术之一。在文献中存 在许多关于区块链支持的供应链可追溯性的综述论文。

文献[18]将 RFID 与区块链技术应用于农业食品供应链追溯，旨在提高食品安全、减 少物流过程中的损失，被称为“农场到餐桌”的解决方案。后续又提出基于 HACCP 的 食品供应链可追溯性的区块链解决方案，以确保在产品的生产、运输和保存过程中符合 HACCP 原则和要求[19]。文献[20]提出了一种基于区块链的用于大豆供应链跟踪的系统，使

用 Ethereum（以太坊）和智能合约来实现对大豆供应链的追踪，详细介绍了基于区块链 的系统架构、序列图和算法。文献[21]提出了一个基于区块链和边缘计算的有机食品供应 信息管理框架，实现了一个基于区块链的数据共享模型，以确保可追溯性记录的不变性。 边缘计算用于降低数据处理成本，提高平均响应时间。文献[22]提出将物联网、机器学习 和区块链技术用于农药产品的反向链。文献[23]提出了一个具有成本效益的信贷系统，允 许相关的农民购买高质量的农产品。为了确保最佳的分级， 该系统包括一个基于分数的 农场-食品质量保证模块。使用以太坊区块链和智能合约来维护信任、透明度和可追溯性。 文献[24]指出在农产品收获前和收获后使用区块链和智能合约与物联网设备集成的区别。

同时提出了一个基于区块链的溯源系统，使用物联网设备在现场收集数据，智能合约控 制所有利益相关者之间的交互。文献[25]提出了一个基于区块链技术和物联网的可跟踪系 统。该系统可以提高食品的可追溯性，提高公众对食品安全和质量控制的意识。文献[26] 提出了一个基于联盟区块链和智能合同的跟踪和追踪农产品的框架。农民使用 IPFS （Inter Planetary File System）记录环境细节和作物生长数据，然后在智能合约中存储 IPFS 散列，提高数据安全性，缓解区块链存储爆炸问题。文献[27] 中描述了一种链上和链 外可追溯性信息的双存储结构，以减轻链负载应变，实现有效的信息查询。该系统提高 了查询效率和数据安全性，保证了数据管理的有效性和可靠性，满足了实际的应用需求。 文献[28]提出了一个分散的 NFC 支持的反假冒系统，以促进葡萄酒行业中可靠的数据来源 的检索、验证和管理。文献[29]提出了一种基于 RFID 和区块链技术的农业食品供应链跟 踪系统，提高了农业食品跟踪信息的可靠性。但该系统存在成本高、数据隐私泄露、存 储容量大等问题。文献[30] 提出并实施了基于区块链和 EPCIS（Electronic Product Code Information Services Standard）的食品安全跟踪系统，并采用链上和链外数据的动态管理 来解决区块链上的数据爆炸问题。文献[31]提出了一种基于 Hyperledger Sawtooth 的通用 农业食品供应链追溯系统。消费者可以通过使用二维码轻松地获取可追溯和可验证的产 品信息。但是， 系统中没有讨论隐私数据保护，Hyperledger Sawtooth 平台的成熟度相对 较低。文献[32]提出基于以太坊平台设计食品可追溯系统，设计双存储模型，将完整数据 存储在本地数据库和区块链中可追溯信息的哈希值，从而提高区块链的运行效率，解决 区块链的可扩展性问题。文献[33]提出了一个基于区块链和 QR（快速响应）代码的框架， 用于数字化食品生产信息和检索，从而使其易于访问、可追溯和可被消费者和生产商验 证。该框架在云中大规模实现， 可以提高区块链的存储容量，并根据消费者的需求提供 灵活的可伸缩性。然而， 如果该农场每天生产超过 1 万个项目，该框架将需要一个更强 大的云服务器，这可能会导致成本的增加。文献[34]使用了几种先进的技术，包括区块链 技术、云计算、二维码和强化学习，共同开发了一个框架，可以有效地减少食物浪费。 文献[35]针对农产品追溯系统中的安全和效率问题，提出了一种基于联盟链的有效解决方 案。文献[36]利用区块链技术设计了茶叶质量安全追溯系统。文献[37]提出了基于区块链的

数字资产交易模型和基于交易链的混合索引机制。

但是，上述研究在存储容量和可伸缩性问题方面仍不完善，仍然存在企业敏感数据 泄漏的风险。文献[38]设计了一个双存储模型，以缓解区块链的存储压力，提高查询速度， 提高系统的灵活性。此外， 还提出了一种数据隐私保护解决方案，以防止利益相关者之 间的信息交互过程中企业敏感信息披露。最后， 对所提出的可跟踪性系统进行了实施和 测试，并进行了详细的分析。

1.2.3 国内外研究现状总结

农产品追溯是追踪农产品从生产到消费全过程的关键信息，通过它可以实现，消费 者获取其消费的农产品的来源信息，监管机构快速识别问题农产品环节，识别责任方， 及时召回问题产品，最大限度地减少损失。然而， 农产品的供应链十分复杂，使得农业 安全监督和可追溯性在实践中极具挑战性。现有的大部分可追溯性系统由第三方管理和 维护，是集中式的体系结构，如企业或政府机构。这就导致了诸如不安全的数据存储、 低可追溯性、低可靠性和数据隐私等问题。区块链可以为农产品供应链中使用的传感器 产生的大量数据提供一个安全的访问环境。然而，区块链技术也面临着新的技术挑战， 包括交易处理能力和安全性等。此外， 由于区块链上的数据都是公开和透明的，这可能 会导致企业的私有和敏感信息泄露。因此， 直接在区块链上处理和存储农产品供应链信 息具有挑战性。

因此，本文将区块链与农产品追溯相结合，以确保农产品数据来源的安全性、可追 溯性和不变性。同时针对区块链交易速度慢和隐私泄漏等问题， 设计了一个改进的共识 算法。

1.3 研究内容和技术路线

1.3.1 研究内容

本文针对当前农产品溯源系统存在的部分问题，提出一种基于区块链的农产品溯源 方案。具体的研究内容包括：

1）设计基于区块链的农产品溯源方案并构建模型。

鉴于现有农产品追溯系统存在的问题，例如数据不公开、不透明、不对称， 掌握在 核心企业的数据容易被篡改等问题，提出一个基于联盟链和智能合约的农产品供应链追 踪方案和模型，结合农产品供应链的全过程，定制化设计数据管理模式和智能合约，以 确保农产品生产和流通信息的公开透明。

2）提出基于分组和信用投票的实用拜占庭容错改进算法。

针对联盟链 PBFT（Practical Byzantine Fault Tolerance）共识算法通信复杂度高、主 节点选择随机、支持的网络规模有限等问题， 提出一种基于分组和信用投票的改进拜占 庭容错算法优化大规模联盟链的节点结构。首先， 优化一致性过程，将网络节点按照对 管理节点的响应速度划分为不同的分组，分别进行组内外共识，减少节点间通信频率， 在此基础上，引入信用模型和投票机制选择管理节点，降低异常节点成为主节点的可能， 提高系统安全。

3）实现基于区块链的农产品溯源系统。

以有机大米的销售为背景，分析系统需求、系统功能等， 进行概要设计，最后使用 超级账本框架实现有机大米溯源，并对系统性能进行测试，以确保其实用性，实现从“农 场到餐桌”的信息可追溯和可共享。

1.3.2 技术路线

本文技术路线如下图 1-1 所示。



图 1-1 技术路线图

Figure 1-1 Technology roadmap

1.4 论文组织结构

本文一共分为六个章节，每章的主要内容如下：

第 1 章，绪论。详细介绍了本文的研究背景及意义， 分析了国内外农产品溯源和区 块链溯源的研究发展现状。最后介绍本文的研究内容，对论文组织结构进行阐述。

第2章，相关理论与技术。介绍了区块链技术和农产品追溯相关技术的发展历程， 涵盖了区块链平台、共识算法、智能合约等常用技术， 以及 IPFS、农产品供应链管理等 与农产品追溯相关的技术。

第3章，基于区块链的溯源方案设计及模型构建。详细描述了本研究提出的基于区 块链的农产品追溯方案的设计和模型构建。通过对传统农产品追溯流程的分析， 设计了 基于区块链的追溯方案，包括选择区块链平台、设计智能合约以及数据存储方案。在此 基础上，构建了基于区块链的农产品追溯模型。

第 4 章，基于大规模溯源的 PBFT 算法优化。结合实用拜占庭容错算法和农产品溯 源的特征对实用拜占庭算法进行了改进，在 PBFT 算法中增加了分组策略、信用模型以 及投票机制，通过实验验证可知，改进后的 PBFT 共识算法为农产品溯源提供了更小的 延迟、更高的吞吐量， 可以支持更大规模的追溯，有效地改善网络节点间通信量急剧增 加的问题，减少恶意节点的影响。

第 5 章，农产品溯源系统的应用实现。根据前面提出的溯源方案、模型以及改进的 PBFT 算法进行农产品溯源系统的实现。首先分析系统角色的需求，依照系统功能分析、 概要设计等依次进行系统实现。

第 6 章，结论与展望。总结本文工作，提出下一步工作展望。

第 2 章 区块链相关理论与关键技术

2.1 区块链技术

2.1.1 区块链概念

区块链技术起源于比特币，2008 年由一位名为“中本聪”的学者提出[39]，本质上 是一个分布式数据库，整合了分布式计算、密码学、网络传输等技术，具有去中心

化、防篡改、可编程和可追溯等特点[40]。就像其名字所描述的，区块链是将区块按照时 间的顺序连接起来，每个区块存储了一个可变大小的事务列表。区块链上的所有数据 都是公开的，各个节点可以生成、读取事务以及参与共识的达成。共识协议是指节点 就哪些事务、哪种顺序组成一个区块。区块链的结构图如图 2-1 所示。区块头主要由 区块号、父区块哈希、时间戳、Merkle 根等信息构成；而区块主体一般包括一系列交 易列表[41]。

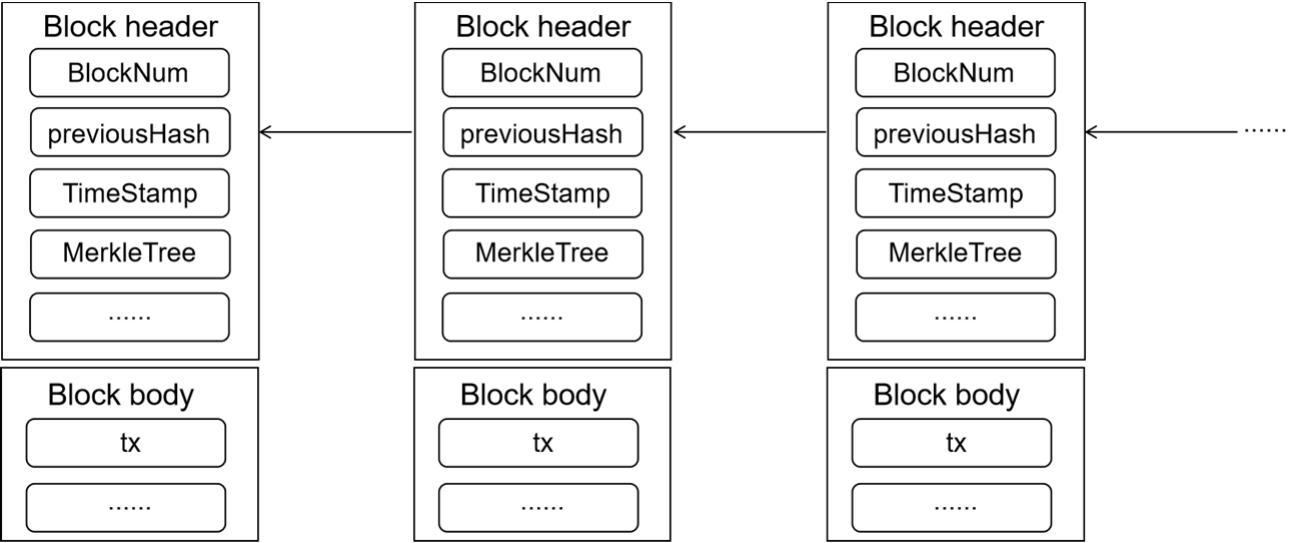


图 2-1 区块链结构简图

Figure 2-1 Blockchain structure sketch

一个区块一旦被足够数量的节点确认（验证通过），它就成为区块链有效且永久 的部分。区块链中还使用到了非对称加密、哈希函数、时间戳和 Merkle 树等技术，使 区块链上的数据更加安全、可靠，使得区块链节点之间的数据传输得到保证，形成透 明的信任机制，消除了对传统集中式机构的依赖[42]。

2.1.2 区块链分类

区块链根据节点准入机制的不同，分为公有链、私有链和联盟链，表 2-1 比较了

三种类型区块链的区别。

公有链如比特币和以太坊，对所有节点开放，是完全去中心化的。公有链上的节 点可以自由地加入或退出网络，随着应用场景的不断扩展，越来越多的领域需要区块 链来实现不完全的去中心化，因此，出现了私有链和联盟链。

表 2-1 三种类型区块链的特征对比

Table 2-1 Comparison of the characteristics of the three types of blockchains

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 类型 | 记账人 | 参与者 | 中心化程度 | 激励机制 | 共识算法 |
| 公有链 | 所有参与者 | 任何人自由进出 | 去中心化 | 需要 | POW/POS/DPOS |
| 私有链 | 自定义 | 个体或公司内部 | (多)中心化 | 可选 | PBFT/RAFT |
| 联盟链 | 联盟成员协商 | 联盟成员 | 多中心化 | 可选 | PBFT/RAFT |

私有链供个人使用，一般不对外开放，存在一定程度的中心化，具有访问权限可 控、交易速度高、成本低等优点[3]。

联盟链由一些组织共同维护，通常每个节点对应一个实体组织，经过身份验证和 授权，可以连接、访问、提交信息，链上的成员可以被赋予不同的数据权限，实现多 家公司或机构的合作[42, 43]。具有成本低、效率高等优点，是当前区块链的主流方向。

2.2 智能合约

在区块链网络中，用户可以部署被称为智能合约的协议[44] 。一般来说，智能合约是 一种实现合约条款的计算机交易协议，在区块链上运行的计算机程序，这些程序在一组 预定义条件的情况下自动或者强制由某些特定的节点执行，可以被认为是传统合同的数 字化版本[45, 46]。

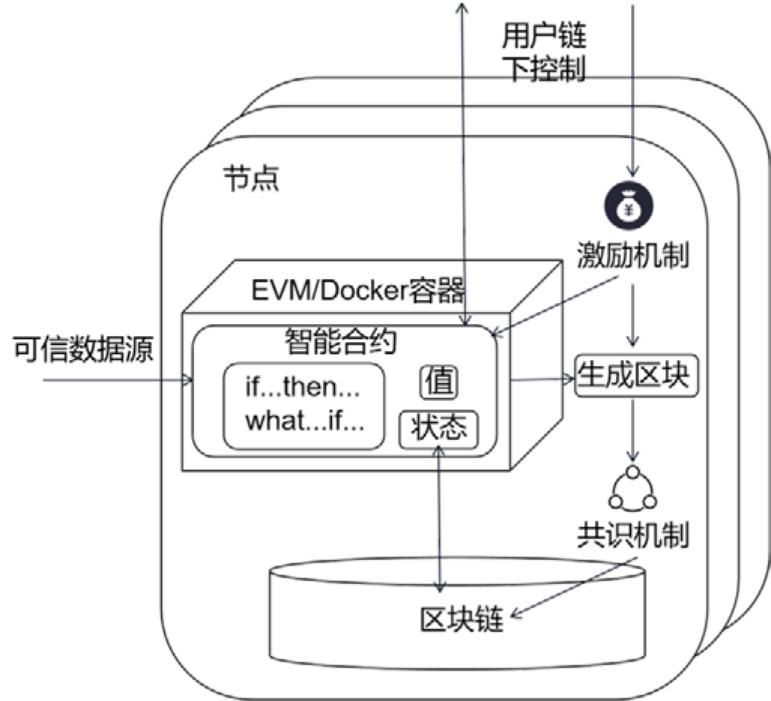


图 2-2 智能合约的运行原理

Figure 2-2 Principle of operation of smart contracts

智能合约由程序代码和存储文件组成。任何用户都可以通过将交易记录写入区块链 来创建合同，消除了对可信中介的需要，在区块链网络中提供了额外的功能，促进了交 易的信誉、自动化和效率[47]。合约的程序代码在创建时是固定的，不能更改，但允许一 个合约调用另外一个合约。以太坊是第一个引入智能合约的区块链平台，支持图灵完备 的脚本语言，允许使用复杂的逻辑编写智能合约。智能合约通常具有两个属性： 值和状 态。代码中使用类似于"If-Then"和"What-If"等语句来预置合约条款的相应触发场景和响 应规则。用户可以通过发起交易来调用合约。在双方都同意并签署后， 通过 P2P 网络传 播，由矿工验证并存储在区块链上的特定区块中。智能合约的运行原理如图 2-2 所示。

2.3 共识算法

共识算法的研究在区块链技术出现之前就已经开始了，作为区块链的核心，主要负 责确保数据传递和处理过程中的正确性和一致性[48, 49] 。具体来说，在本地节点上保存相 同的账本信息，以避免数据篡改，并能够在一致性协议过程中快速检测数据是否被更改， 从而有效保证数据的安全性。

根据系统能否解决拜占庭错误可将共识算法分为崩溃容错协议（ Crash Fault Tolerance ，CFT）和拜占庭容错协议（Byzantine Fault Tolerance ，BFT）两大类[50] 。CFT 类共识算法无法应对拜占庭错误，主要应用于私有链中；BFT 类共识算法可以应对拜占 庭错误，被广泛应用于公有链和联盟链中[51, 52] 。BFT 类的共识算法有工作量证明（Proof of Work ，PoW）、权益证明（Proof ofStake ，PoS）、委托权益证明（Delegated proofof of Sequi，DPoS）和实用拜占庭容错（Practical Byzantine Fault Tolerance，PBFT）等[53-56] 。 PoW 主要通过计算机算力对 SHA-256 密码散列函数进行运算，该算法不但计算量大， 而且共识效率较低[57] 。PoS 算法的出现是试图解决 PoW 机制中大量资源被浪费的情况， 通过计算持有占总币数的百分比，以及占有币数的时间来决定记账权[58]。该算法在一定 程度上克服了大量算力的缺点，但存在资源分布不均匀、持币趋于集中化且流动性较差 等缺点[59] 。DPoS 机制是在 PoS 基础上优化而来的，节点通过投票选举的方式，选出生 产者，代表他们履行权利和义务，提高了区块生成的效率，但也偏离了去中心化的原则。 以上算法在一定程度上可以保证区块链的可靠性，但都有各自的短板，不能同时解决时 延、吞吐量和安全性等问题。 PBFT 共识算法是 Castro 等基于 BFT 算法改进的，用于解 决 BFT 算法计算量大的问题，将算法复杂度从指数级降到了多项式级，并且在有一定数 量的拜占庭节点情况下仍能使分布式节点达成共识，是公认解决拜占庭将军问题最优的 算法[60, 61]。然而，PBFT 算法也存在主节点选取方式随意、三阶段协议通信复杂度较高、 节点不能动态加入、退出等问题，降低了联盟链的性能。

2.4 超级账本 Hyperledger Fabric

超级账本（Hyperledger Fabric）是一个由IBM 和 Linux 基金会共同维护的企业级开 源平台。通过成员服务提供者（Membership Service Provider ，MSP）进行成员身份管理 和验证的。与比特币和以太坊不同， Hyperledger Fabric 不涉及任何加密货币，数据的访 问仅限于网络成员[62]，属于联盟链。Hyperledger Fabric 采用模块化架构，具备极佳的保 密性、可伸缩性、灵活性和可扩展性， 支持不同的模块组件的插拔使用，并能适应溯源 等各种复杂场景的。

2.5 IPFS 技术

IPFS（InterPlanetary File System，星际文件系统）是一种分布式文件系统，它集成 并利用了诸如 DHT（Distributed Hash Table, 分布式散列表）、Git（分布式版本控制系 统）、P2P（对等网络传输）、BitTorrent（比特流，一种内容分发协议）和加密技术等 技术，旨在创建一个全球范围的、点对点的文件共享网络， 基于点对点协议，具有可靠 性、高效性和安全性等特点。

在 IPFS 系统中，文件将被分割成 256K 个单元块，数据以块的形式存储，每个块将 计算一个块哈希值。为了获得唯一的文件标识符 CID（内容 ID），所有的块散列值都被 组合和散列。相应存储文件的 CID 和节点 ID 记录在 DHT 上，用户可以单独使用 CID 在 IPFS 网络中下载相应的文件。由于 IPFS 是一种基于内容寻址和哈希算法的分布式文 件系统，因此 IPFS 中的文件数据是不可变的，具有很强的防篡改能力。

IPFS 网络中的任何节点都是独立的，不需要信任其他节点，因此不像传统的 HTTP （超文本传输协议）传输中那样存在单点故障。当用户在 IPFS 中存储一个文件时，IPFS 会由于数据存储而生成一个 32 位的散列。IPFS 的点对点传输可以显著降低网络带宽消 耗，分布式文件可以显著降低 DDoS（Distributed Denial of Service, 分布式拒绝服务）攻 击的风险。

IPFS 的核心思想是使用哈希作为文件的唯一标识符，将文件分块并分散存储在网 络上的多个节点中，这些节点可以是用户自己的计算机，也可以是专门提供存储服务的 计算机。用户可以通过哈希值来访问文件， 而不是通过文件的物理位置。IPFS 也具有版 本控制功能，因为每个文件都有唯一的哈希值，用户可以创建多个版本的文件并存储在 IPFS 网络中，从而实现分布式的版本控制。IPFS 还提供了一个名为 IPNS（InterPlanetary Name System）的命名系统，用于将可变的、易变的字符串名称映射到不变的、唯一的 IPFS 哈希值。IPFS 被认为是 Web 3.0 的核心技术之一，可以用于构建分布式应用程序、

实现去中心化的数据存储和访问等。

2.6 本章小结

本章阐述了区块链的相关理论及关键技术。首先介绍了区块链相关的技术， 包括区 块链概念、分类，使用的区块链开源平台 Hyperledger Fabric、共识机制和智能合约等， 最后阐述了农产品溯源所涉及的 IPFS 存储技术，为下一步的研究工作奠定基础。

第 3 章 基于区块链的溯源方案设计及模型构建

3.1 传统农产品溯源方案分析

传统农产品追溯是指记录农产品的供应过程，通过标识供应链上农产品位置等方式 方便对农产品进行追溯[63]，从而检查产品的安全和对其质量进行控制。参与农产品生产 流程的人员包括生产者、加工厂、分销商、零售商以及消费者， 物流参与在供应链的各 个环节之间。

随着信息技术的发展和信息化溯源平台的出现，越来越多的企业采用中心化溯源系 统记录农产品的流转过程。这些系统按照农产品生产流程严格记录农产品在不同环节的 重要数据，为农产品溯源提供了可靠的数据保障。这些平台大多由企业自行搭建或者使 用第三方溯源平台。图 3-1 展示了传统中心化溯源的模式。

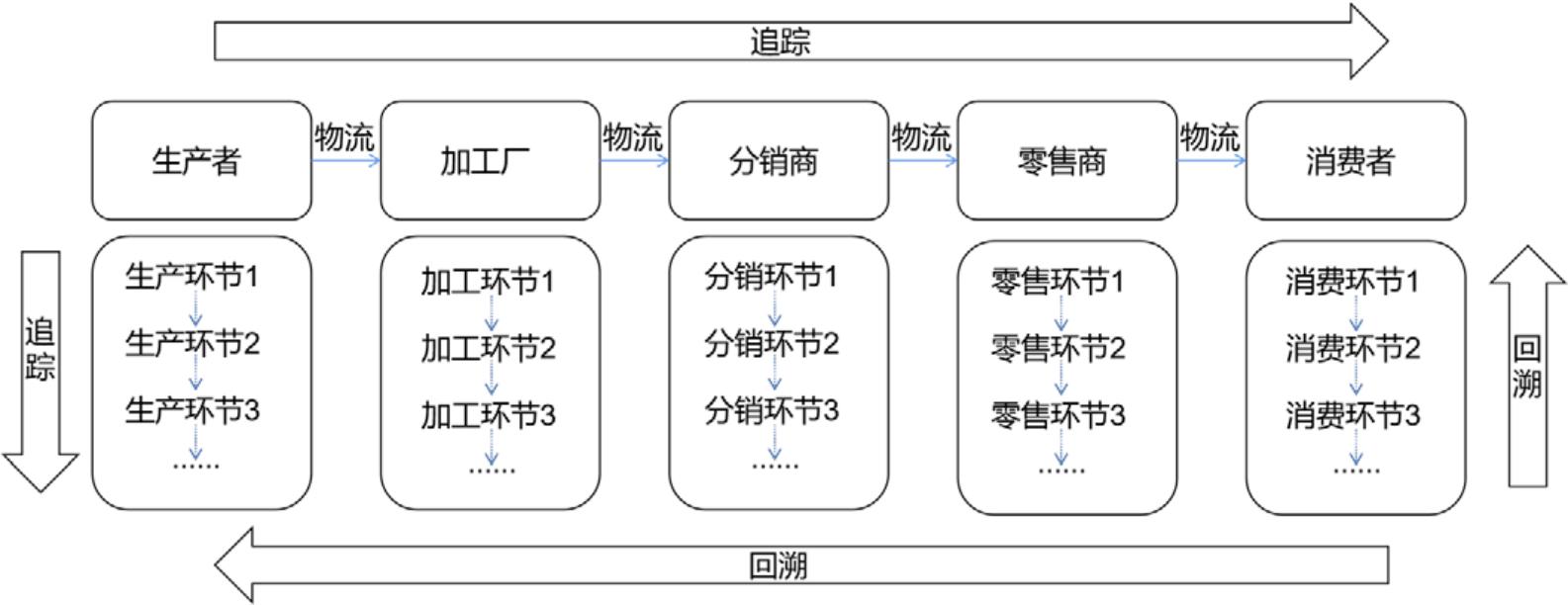


图 3-1 农产品中心化溯源模式

Figure 3-1 Agricultural products centralized traceability model

中心化的农产品溯源平台在某种程度上解决了农产品溯源信息传播的问题，然而， 只要具备操作权限，任何企业或个人都可以登录系统查询农产品信息。在这些平台上， 产品溯源信息存储在中心化数据库中，因此数据安全性难以保证[64]。

3.2 基于区块链的溯源流程分析

传统的农产品追溯系统是集中式的，通常由企业自行管理，这意味着很容易遇到单 点系统故障、数据篡改、系统维护困难等问题。相比之下， 本文提出的基于区块链的农 产品溯源系统本质上是去中心化的，所有区块链节点都以协作的方式维护数据。其次，

传统农产品系统将溯源信息存储在各自的本地数据库中，容易造成数据丢失和形成“信 息孤岛”。本文提出的溯源模型， 其中完整的可追溯性信息存储在中心数据库的链下，而 关键信息存储在区块链的链上，确保数据不易丢失并保持真实性。第三， 由于传统农产 品追溯系统的集中管理，在利益的驱使下，企业可能存在未经授权更改农产品追溯信息 的问题，容易导致信息造假。 同时，中心化数据库很容易受到网络的攻击。在本文中， 提出的一种使用区块链技术的农产品追溯系统，其中存储在区块链中的任何数据都不能 被篡改。因此，可以保证该系统中可追溯性的可靠性。最后，在发生农产品安全事故时， 对传统农产品追溯体系的审核更加繁琐、难度较大。区块链是一个去中心化的分布式账 本，所有用户的操作和交易都会被记录下来，不能被篡改，一旦交易完成，任何用户都 不能否认它发起的操作。因此，所提出的系统可以轻松跟踪和审核每个参与者的行为。

为了解决传统农产品溯源中存在的问题，设计了一个基于区块链技术的农产品溯源 方案。该方案从供应链的各个环节出发， 分析了区块链的应用方式，并通过区块链共识 算法、智能合约等关键技术协同配合， 实现了各流通环节中溯源数据的无缝连接，从而 确保了信息在传递过程中的完整性和可信性。具体流程图如图 3-2 所示。

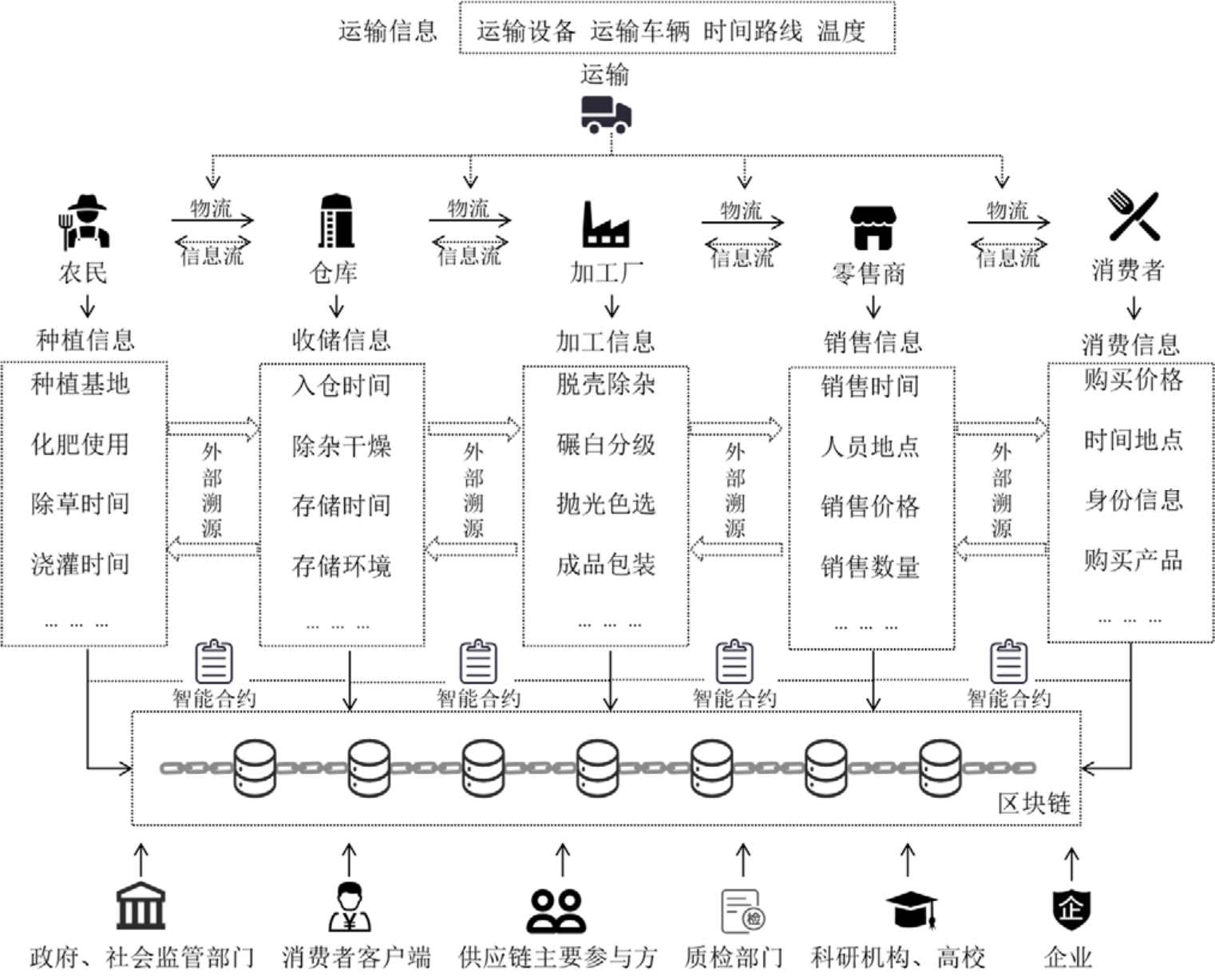


图 3-2 农产品供应链溯源流程

Figure 3-2 Traceability process of agricultural product supply chain

农产品溯源过程信息非常复杂和多样化，选择供应链中哪些关键环节的信息安全上 链是一个重要而困难的问题。与其他溯源体系不同， 农产品溯源体系的复杂性在于种植

过程，而精确的种植记录是确保食品安全的有力保障。举例来说， 如果某批化肥被检测 出不合格，以往可能需要几天甚至几周时间才能查明哪几批农产品受到了污染，但是如 果种植信息一旦上链，解决上述问题将变得简单且迅速。在农产品供应链中， 主要参与 的实体包括农民、存储仓、加工厂、零售商、最终客户。每个实体的描述如下：

1）农民：使用种子生产大量秧苗，秧苗的生长种植环境，包括土壤、阳光、水、空 气、温度等都需要一一记录，该过程为采取合理的措施来确保农产品生长的安全性，应 提供相关的监测数据，定期监控、记录生长细节， 还需要记录施用的肥料、除草剂和杀 虫剂的种类以及用量。收获过程，要注意记录采摘时间、操作的员工或者机器等。

2）仓库：从农民处购买农产品，由仓库管理员及相关测量仪器决定农产品的质量等 级。在储存时要考虑温度、湿度、储存时间等因素。

3）加工厂：加工处理环节，要对农产品进行干燥、筛选、去石、去壳、谷糙分离、 分级、抛光、成品包装等处理， 很可能发生在不同的地点，需要对加工环境和设备进行 评估。在最后的包装过程应严格监控打印的生产日期、生产批号等。

4）零售商：从加工厂购买最终产品，向消费者出售，使用传感器(如全球定位系统) 可以监测运输的路径，查看产地。出售前， 需要检查农产品的质量及生产日期，确保及 时更换过期产品。

5）消费者：从零售商处购买和消费农产品的最终用户，能够通过包装袋上的溯源 码，查询农产品的溯源信息。

通过基于区块链的溯源应用环节设计，可以保证溯源系统的去中心化、信息公开透 明性和产品可信溯源性。然而， 由于供应链涉及的环节较多且整体长度较长，为确保产 品信息的高效和准确同步，同时降低溯源系统的通信开销，需要采用更高效的共识算法 进行信息的同步和存储。因此，本文将在第 4 章对区块链的共识算法进行改进研究。

3.3 基于区块链的溯源方案设计

3.3.1 区块链平台选择

区块链 1.0 是以比特币为代表，是一种去中心化的数字货币区块链系统，而 2.0 则 引入了智能合约的概念[65]。在区块链 2.0 中，可用于跟踪的区块链框架有很多，要明确 的是，在不同的业务场景下，区块链类型的选择也不尽相同，区块链分为公有链、私有 链和联盟链，选择使用哪种区块链技术以及如何使用区块链技术是整个系统的关键。 Linux 基金会的 Hyperledger Fabric 和 Vitalik Buterin 领导的以太坊基金会的 Ethereum 是 两个现阶段使用较广泛的平台[66]。这两种区块链系统具有截然不同的设计思路。Ethereum

侧重区块链原本的思维设计模式，与比特币类似；Fabric 更偏向企业信息系统思维的设 计模式[67, 68]。

针对课题研究背景，由于溯源过程中牵涉到不同节点的参与，且需要不同单位的不 同节点加入，考虑到公有链的共识算法可能会浪费大量资源，因此基于区块链的农产品 溯源系统应当建立一个联盟链。在该联盟链中， 个人或组织只能在被授权认证之后才能 加入系统，避免了采用 PoW 共识算法（Ethereum）的资源浪费，并大幅提高了交易处理 效率，满足系统对处理性能的需求。

Hyperledger Fabric 是联盟链的代表。同时， Hyperledger Fabric 采用模块化的设计理 念，将权限认证模块、共识服务模块、背书模块和区块提交模块等进行分离部署。开发 者可以根据具体的业务场景进行模块替换，实现了插件式管理。此外，Fabric 使用 Docker 机制实现智能合约。这使得 Fabric 可以使用多种编程语言来开发智能合约，如 Java、Go 、 NodeJS 等，并可以调用多种库函数和系统函数，因此使用门槛相对于 Ethereum 的专用 编程语言（solidity）较低。除此之外，Channel 的概念是 Hyperledger Fabric 所特有的， Channel 的引入，使得 Fabric 的智能合约是直接部署在某几个节点上的，为在同一系统 中运行的不同利益相关者提供了业务逻辑和数据隐私安全。除了上面将描述的特性外， Hyperledger Fabric 已被证实提供卓越的交易吞吐量， 最高可达每秒几千笔交易，使 Hyperledger Fabric 成为复杂供应链系统的完美候选。

3.3.2 智能合约设计

智能合约的核心设计思想是在满足一定条件下自动执行，即基本满足 if……then 或 what……if的逻辑。同时，智能合约必须在链上进行部署和编译，才能实现对节点的读 写操作[9, 69]。通过智能合约，系统自动判断农产品的销售是否符合要求。

算法 1 描述农民向仓库销售农产品的过程。智能合约由农民创建。在建立智能合同 的初始状态下，首先检查农民是否注册。然后， 仓库相关人员发出购买请求，此时合同 状态为 Generated，需要检查两个条件：1）农民和仓库为注册实体；2）农产品的销售已 经达成协议，并支付了价格。如果这 两个条件满足，则合同状态更改为 AgriculturalproductsRequestMade，仓库状态为 WaitForAgriculturalproductsFromFarmer ， 农民状态更改为 SellAgriculturalproductsToGranary，所有活动实体都会从农民处收到有 关出售给仓库农产品的信息。如果不满足上述两个条件，则合同状态将变为 AgriculturalproductsRequestFailed ， 仓 库 状 态 为 RequestFailed ， farmer 状 态 为 CancelRequestOfGranary。

|  |
| --- |
| **算法 1.** 农户向仓库出售农产品 |
| **输入:** ‘G’ 为已注册的仓库  仓库节点的地址 农户节点的地址  质量, 购买日期, 购买价格  1 合约状态为 **Generated**  2 仓库状态为 **AgriculturalproductsRequested**  3 农户状态为 **Prepared**  4 需要满足条件 G ∈ 仓库  5 **If** 农户= 已注册 and 达成交易协议 and 已支付购买价格, **then**  6 合约状态改为 AgriculturalproductsRequestMade.  7 仓库状态改为 WaitForAgriculturalproductsFromFarmer.  8 农户状态改为 SellAgriculturalproductsToGranary.  9 创建一个通知信息, 说明农产品的销售情况  10 **End**  11 **Else**  12 合同状态更改为 AgriculturalproductsRequestFailed.  13 仓库状态改为 RequestFailure.  14 农户状态改为 CancelRequestOfGranary.  15 创建一个通知信息, 说明请求失败  16 **End**  17 **Else**  18 返回到合同状态, 并显示错误信息  19 **End** |

算法 2 描述顾客从零售商那里购买农产品，顾客是农产品加工和跟踪模型中的最终 实 体 。 最 初 的 客 户 状 态 是 ReadyToPurchase ， 合 约 和 零 售 商 的 状 态 分 别 是 SaleRequestMadeSuccess 和 AgriculturalproductsDeliveredSuccessful。成功支付购买的农 产品价格后，合约状态改为 AgriculturalproductsSoldToCustomer ，零售商状态改为 SaleofAgriculturalproductsSucessful，客户状态改为 SucessfulPurchase。如果付款不成功， 合 约 状 态 改 为 SaleOfAgriculturalproductsFailed ， 零 售 商 状 态 改 为 AgriculturalproductsSaleFailure，客户状态改为 FailedPurchase。合约将购买失败的事件通 知给网络中的每个节点。

|  |
| --- |
| **算法 2.** 顾客从零售商处购买农产品 |
| **Input:** 零售商节点的地址 顾客节点的地址  购买日期, 农产品编号, 售出编号  1 合约状态为 **SaleRequestMadeSuccess**  2 零售商状态为 **AgriculturalproductsDeliveredSuccessful**  3 顾客状态为 **ReadyToPurchase**  4 **If** 已成功支付购买价格, **then**  5 合约状态改为 AgriculturalproductsSoldToCustomer.  6 零售商状态改为 SaleofAgriculturalproductsSucessful.  7 顾客状态改为 SucessfulPurchase.  8 创建一个通知信息, 说明农产品已完成销售  9 **End**  10 **Else**  11 合约状态改为 SaleOfAgriculturalproductsFailed.  12 零售商状态改为 AgriculturalproductsSaleFailure.  13 顾客状态改为 FailedPurchase.  14 创建一个通知信息, 说明请求失败  15 **End**  16 **Else**  17 返回到合同状态, 并显示错误信息  18 **End** |

3.3.3 数据存储设计

因为区块链透明性这一特征，链上的所有用户节点都可以访问链上信息，使得一 些重要数据的安全性受到了挑战。在农产品生产的过程中，供应链各方都有一些生产 数据是敏感的，无法完全公开，例如企业核心的工艺、技术、金融方面的数据等，不 能直接上传至区块链，需要做一定的处理。本文将上传的数据分为公开数据和隐私数 据，结合链上链下相结合的存储方式，设计隐私数据加密存储模式，将隐私数据采用 哈希算法进行加密并上传至区块链网络。由于哈希算法的单向特性，哈希算法的计算 过程是单向不可逆的，这保证了数据内容不能被数据的哈希值计算出来。此外，由于 哈希算法的抗碰撞特性，一旦提供的数据被篡改或不完整，计算出的哈希值必须发生 变化，导致构建的 Merkle Tree 根节点的哈希值不一致。如图 3-3 所示，链下数据库 MySQL 中存储完整的数据，链上存储完整的公开数据和经过加密的隐私数据。

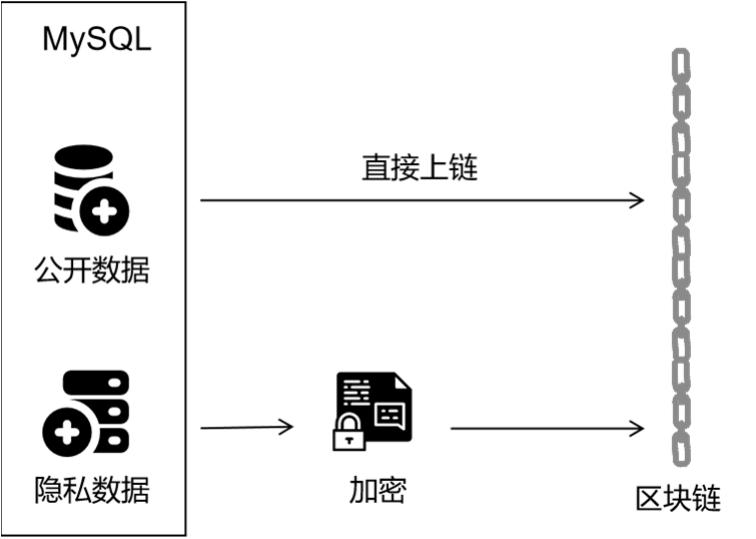


图 3-3 数据管理模式

Figure 3-3 Data management mode

表 3-1 系统溯源数据需求表

Table 3-1 System traceability data requirements table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 实体 | 关键数据 | 采集方式 | 存储类型 | 是否需要加密 |
| 农户 | 农产品品种  种植人员 ID  种植区域 ID  种植方式  种植时间  施肥、除草、杀虫周期 | 条形码采集设备 部门录入  北斗、GPS 定位 种植人员录入 种植人员录入 种植人员录入 | varchar(10)  int  int  varchar(10)  datetime  int | 否 否 否 否 否 否 |
| 存储仓 | 售出价格 | 调用智能合约录入 | int | 是 |
| 仓库 ID 出入库时间 售出价格 | 部门录入  部门录入  调用智能合约录入 | int  datetime  int | 否 否 是 |
| 负责人员 ID 加工车间 ID  操作(干燥、筛选、去石、去壳、 | 部门录入 部门录入 | int int | 否 否 |
| 加工厂 | 谷糙分离、分级、抛光、成品包  装)等参数 生产工时 质检结果 售出价格 | 负责人录入  负责人录入  负责人录入  调用智能合约录入 | varchar(50)  int  varchar(10)  int | 是 否 否 是 |
| 销售地点 | 销售人员录入 | varchar(50) | 否 |
| 零售商  运输商 | 销售人员 ID 售出价格 | 部门录入  调用智能合约录入 | int int | 否 是 |
| 物流编号  车辆/员工 ID 经过地经纬度 | 员工录入  部门录入  北斗、GPS 定位 | int  int  float | 否 否 否 |

农产品供应链上五类参与人员涉及溯源的众多环节，各个环节都包含对数据的添加、 删除、修改以及查询等操作，因此需要选择关键的数据上链，减少信息冗余性，表 3-1 描述了农产品供应链各个参与主体需要上链的关键数据、数据的采集方式、存储类型以 及该数据是否需要加密等信息。

3.4 基于区块链的溯源模型构建

经过对农产品供应链溯源方案的分析以及溯源流程和方案的设计，我们构建了一个 农产品溯源的模型。通过该模型， 系统可以保证可追溯信息的完整性和真实性，企业不 必担心数据隐私问题，同时可以实现细粒度的可追溯性和信息共享，如图 3-4 所示。该 模型的详细设计如下。

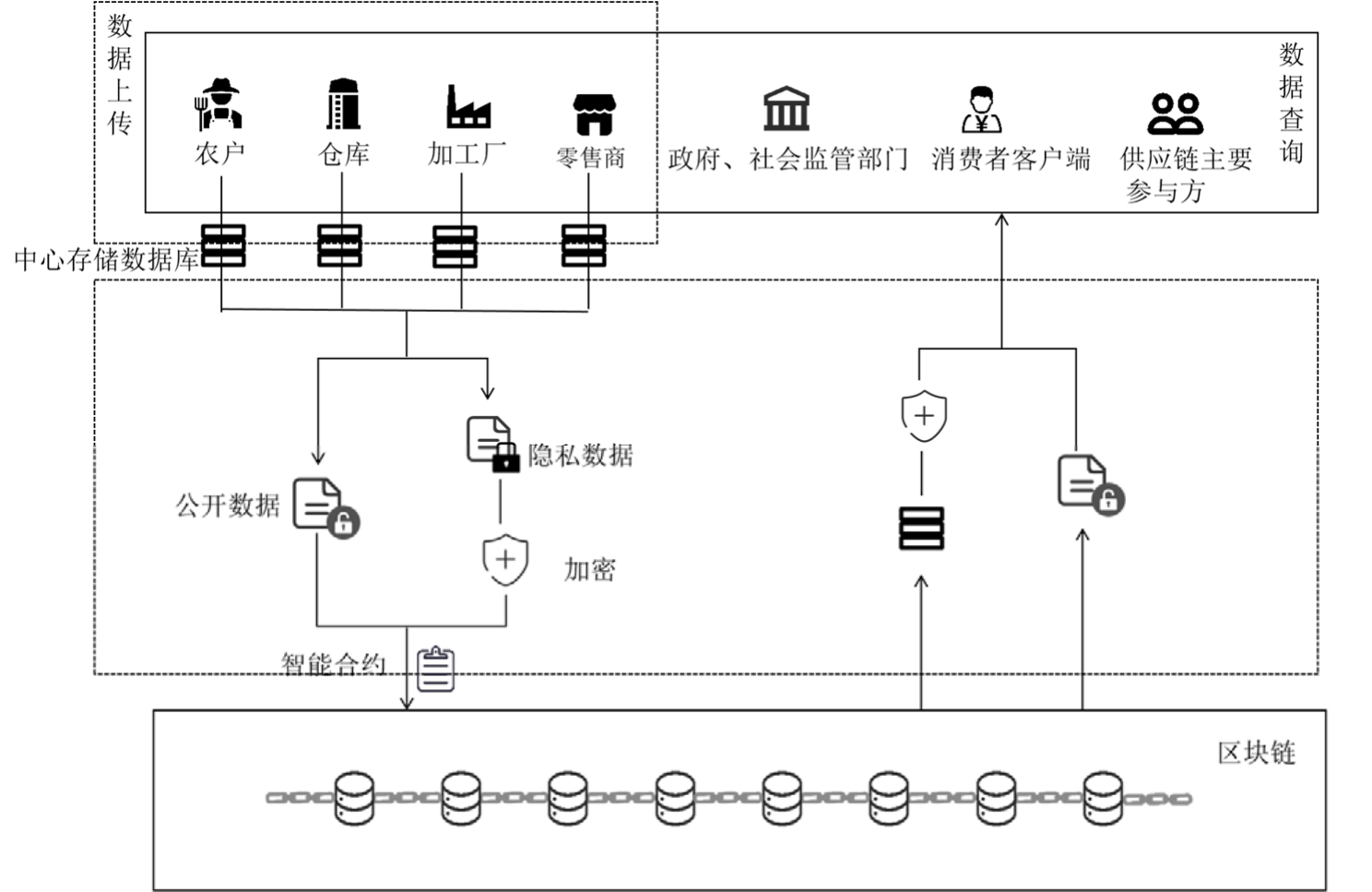


图 3-4 基于区块链的农产品溯源模型

Figure 3-4 Traceability model of agricultural products based on blockchain

安全可靠的农产品追溯体系，覆盖农产品供应链中的生产、加工、仓储、物流、销 售全过程[70, 71]。参与实体包括农户、存储仓、加工厂、物流供应商、零售商和消费者。每 个参与者的业务都在监管机构的有效监督下进行。监管机构负责各主体农产品质量安全 事件的身份认证、权限管理、数据监管、追溯等工作。

为了实现农产品供应链的安全追溯，数据被存储在区块链系统和 MySQL 数据库中。 引入关系数据库可以解决区块链系统的隐私问题。只有隐私数据的加密形式存储在区块 链系统中，完整的数据存储在 MySQL 数据库中。数据库由个人公司维护，区块链系统 由农户、存储仓、加工厂、物流供应商、零售商、工商行政管理部门、食品监督管理局

等共同维护。

农户、存储仓、加工厂、物流供应商、零售商的信息录入流程相同。以加工厂为例， 加工厂将农产品加工过程中采集到的数据打包，同时输入到节点和数据库中。加工厂的 隐私数据使用哈希加密生成密文，并将其发送到区块链。达成共识后， 参与节点将隐私 数据密文写入区块。

购买食品的消费者可以使用农产品包装上的溯源码进行溯源查询。如果对查询到的 信息有疑问，消费者可以向工商行政管理部门投诉。该部门将查询和比较区块链中的信 息摘要，以确定数据是否被更改。如果信息摘要一致，则数据被认为真实且不变。如果 查询数据被更改，投诉信息将以与证据相同的方式存储在数据库和区块链系统中，并向 责任方追究责任。

由于农业供应链各环节收集的数据量较大，信息输入过程中可能会因人为错误或其 他外界干扰而遗漏或记录错误。此外， 一旦信息输入区块链系统，数据就无法更改，因 此将食品管理局引入该方案。如果农业供应链中的任何节点发现输入信息有任何错误， 它可以向食品管理局发送信息更正请求。经食品监督管理局验证后， 更正后的信息可由 节点重新上传到区块链系统。这些方法可以消除人为操作错误造成的信息输入错误的巨 大损失。

基于区块链的农产品追溯方案设计，确保数据不可篡改，去除中心化结构。根据实 际需要，有针对性地引入食品监督管理局、工商行政管理部门等部门。食品监督管理局 不仅能够处理供应链各个阶段的信息输入错误，还可以满足数据更正的需求、召回可能 对人体健康造成损害的问题食物。工商行政管理部门负责及时受理消费者投诉， 对可能 损害消费者健康的投诉信息，将及时与食品监督管理局共享，及时开展食品召回工作。

3.5 本章小结

在本章中，首先对传统农产品溯源方案存在的问题进行了分析。之后根据农产品供 应链的实际需求和区块链的结构特征，设计了一种基于区块链的农产品溯源方案。在此 基础上，通过区块链智能合约、数据库设计等关键技术的协同配合， 实现了各流通环节 中溯源数据的无缝连接，并最终构建了基于区块链的农产品溯源模型。这些设计和构建 工作是区块链农产品溯源平台实现的基础。

第 4 章 基于农产品溯源的 PBFT 算法优化

区块链技术在农产品溯源领域的发展潜力备受青睐，可以利用其特有的特性来改善 农产品供应链的溯源模式，实现农产品信息的全程“可视、可控、可追溯”。除了上述 优势外，区块链共识机制的局限性也给供应链带来了巨大的挑战，随着网络节点的爆炸 式增长，农产品供应链交易和账户数据更新较为频繁，共识算法吞吐量低、交易延迟高、 通信开销大等问题，严重影响了基于区块链溯源系统的整体性能，大多数研究都没有探 索区块链共识机制适应于农产品供应链。因此， 研究实现一种可以满足高吞吐量、低延 时和支持大规模网络的区块链共识机制成为重点。为了解决这一挑战，设计了一种基于 改进 PBFT 的、高效的、支持大规模的农产品溯源共识算法， 以实现区块链农产品溯源 系统的高安全性和低通信开销。

4.1 PBFT 共识算法

Pease 和Lamport 于 1980 年提出了拜占庭容错（BFT）算法，用于解决在有恶意节 点或网络堵塞的点对点网络中如何实现数据一致性和完整性[72]。PBFT 共识算法是 Castro 等人基于 BFT 算法改进的[73]，被认为是解决拜占庭问题的最佳算法之一，并广泛应用于 当前联盟链中分布式系统的共识问题。PBFT 算法继承了BFT 算法的容忍拜占庭节点的 优点，将 BFT 算法中的通信复杂度从O(*n3* ) 降低到了O(*n2* )，共识效率相对较高，启动 节点数量较少，容错率接近 1/3，是联盟链中应用较广泛的共识算法，由一致性协议、 视图更换协议和检查点协议组成。

4.1.1 PBFT 算法的一致性协议

PBFT 被认为是解决拜占庭问题的最佳算法之一，它有三个角色：客户端、主节点 和从节点[74]。客户端提交事务请求后，将立即发送到主节点，主节点在全网发起事务投 票，节点运行一致性协议，通过点对点通信获取信息，使用类似投票的过程完成区块链 数据的统一。从节点和主节点共同维护事务投票的有效性， 当主节点失效，将触发视图 更改程序，选择一个新的主节点[75] 。PBFT 算法流程如图 4-1 所示。

首先，客户端*C* 向主节点0 发送一个消息*m* ，主节点启动 PBFT 的五段协议——请 求、预准备、准备、提交和回复。*C* 表示客户端节点，0~3 表示共识节点，其中，0 是 主节点，3 是故障节点， *σ* 为签名标志。

1）发送请求阶段

客户端节点生成消息摘要，添加请求操作*o* 、时间戳 *t* 构造请求。完成签名后，将 REQUEST,*o,t*,*C**σ C* 发送到主节点。

2）预准备阶段

主节点接收到消息后，构造《PRE−PREPARE,*v,n,d**σ 0 ,m*并广播给从节点，从节点 判断是否满足以下内容，若满足则接收消息：

•检查消息摘要*d* 与*m* 生成的摘要是否一致。

•接收到消息中的*v* 与当前视图是否一致。

•检查本地是否接收到相同的*n* 和*v* ，但不同 *d* 的消息。

3）准备阶段

从节点接收预准备信息，进入准备阶段，向其他节点广播消息 PREPARE,*v,n,d,i**σ i* ， 节点收到准备消息验证是否符合以下要求，接收3*f* +1（包括其自身）个消息即可进入提 交阶段：

•准备消息签名是否正确。

•当前节点是否收到相同*v* 、*n* ，但不同签名的消息。

•判断当前节点生成的摘要，是否与*d* 一致。

4）提交阶段

提交阶段需要广播 COMMIT,*v,n,i* *σ i* ，其他节点判断：

•接收到的消息签名是否正确。

•当前节点在一个*v* 下没有接收到同一个*n* 。

•当前节点生成的信息摘要与收到的*d* 相同。

5）回复阶段

当前节点收到2*f* +1（包括其自身）个提交后，将消息记录到本地日志中并回复客户 端。客户端*C* 收到回复后，整个网络达成了共识，消息提交到本地数据库。

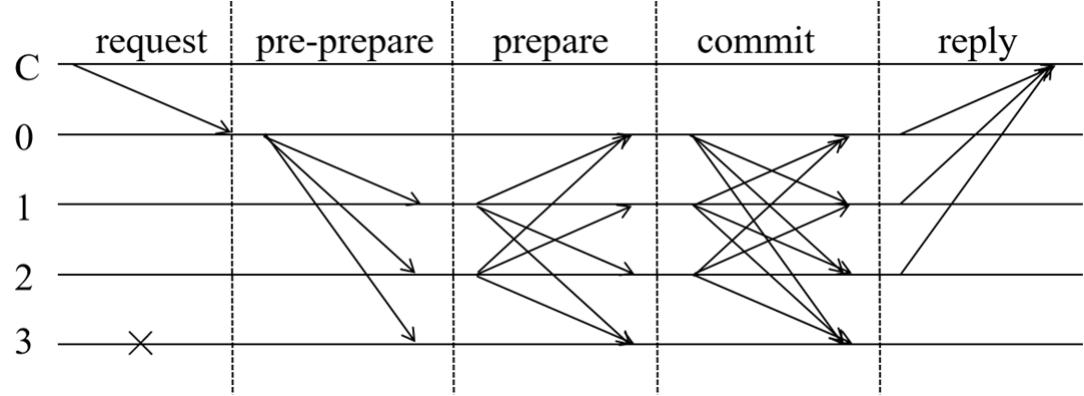


图 4-1 PBFT 算法流程

Figure 4-1 PBFT algorithm flow

4.1.2 PBFT 算法的视图切换协议

PBFT 算法运行一致性协议时，若主节点发生故障，系统会在一定时间内替换故障 节点，改变视图，这个协议就称为视图切换协议[76] 。一个主节点领导的过程处于一个视 图下，视图是连续编号的整数，由公式*P*=*V*mod*R*计算得到，其中： *v* 是视图编号，*P* 为主节点编号，*R*是节点的个数。当发生主节点失效、共识过程超时等情况时， 需要切 换主节点，启动视图切换协议并生成新的视图*v*+1，然后在新视图下继续共识过程。

4.1.3 PBFT 算法的检查点协议

从一致性协议可以看出，系统每执行一个请求，服务器都需要记录日志（request、 pre-prepare 、prepare 、commit）等消息。日志若得不到及时的清理，会导致大量系统资 源被占用。此外， 由于存在拜占庭节点，一致性协议无法保证每台服务器都执行了相同 的请求，因此不同服务器之间可能存在状态不一致的情况。因此， 检查点协议主要作用 有 2 个：定期清理日志，减轻节点存储负担；检查系统状态是否统一，对不一致的节点 进行同步。

4.1.4 PBFT 算法存在的缺陷

尽管 PBFT 共识算法具有明显优势，但该机制仍然存在以下的问题：

1）主节点的选举方式过于随意。在现有的 PBFT 算法中，主节点选举往往会采用轮 替或随机方式在所有节点中进行，这种选取方式容易受到 P2P 网络中的 DDoS 攻击和女 巫攻击的影响，存在较高的安全隐患。

2）投票过程过于复杂。三段式协议广播过程需要进行通信开销极大的全网转发， 给 共识网络带来了过高的负荷[77]。

3）PBFT 共识算法中节点不能随意加入、退出， 影响系统可用性，且采用C/S 架构 无法动态感知节点的数量。随着节点数量的增加， 性能急剧下降，不适用于大规模的动 态网络，限制区块链技术在金融服务、供应链管理、物联网（IoT）等领域的应用。

4）节点缺乏有效奖惩机制，无法奖励诚实节点或惩罚作恶节点，从而导致节点的忠 诚度和积极性较低。

4.2 T-PBFT 算法设计

目前大多数联盟链是基于实用拜占庭容错算法（PBFT）等共识算法实现的，它们通

常局限于时延高、吞吐量低、系统开销大、支持的规模小等一系列问题，是区块链农产 品溯源系统难以广泛使用的一个重要原因[78]。为了解决这一挑战，设计了一种基于改进 PBFT 的、高效的、支持大规模农产品溯源的共识算法，以实现区块链农产品溯源系统 的高安全性和低通信开销。

4.2.1 T-PBFT 算法整体思路

T-PBFT 是一种基于 PBFT 算法改进的安全高效的拜占庭容错共识算法，对比 PBFT 算法主要引进了两个新的阶段，分组阶段与管理节点选举阶段。

1）分组阶段是将大量网络节点根据响应速度划分为多个小组，简化共识的复杂性， 有利于减少网络节点的规模和系统通信量。

2）管理节点选举阶段是以节点的信用值为主要参考，在组内投票选择信用较高的 节点作为管理节点，将单个管理节点扩展为多个管理节点，降低管理节点是拜占庭节点 的概率，提高系统安全性[79] 。假设整个网络的节点数为 *N* ，需要满足每组节点数 *K* ≥3 ， 分组数*G*≥4 。改进算法的主要流程如图 4-2 所示。

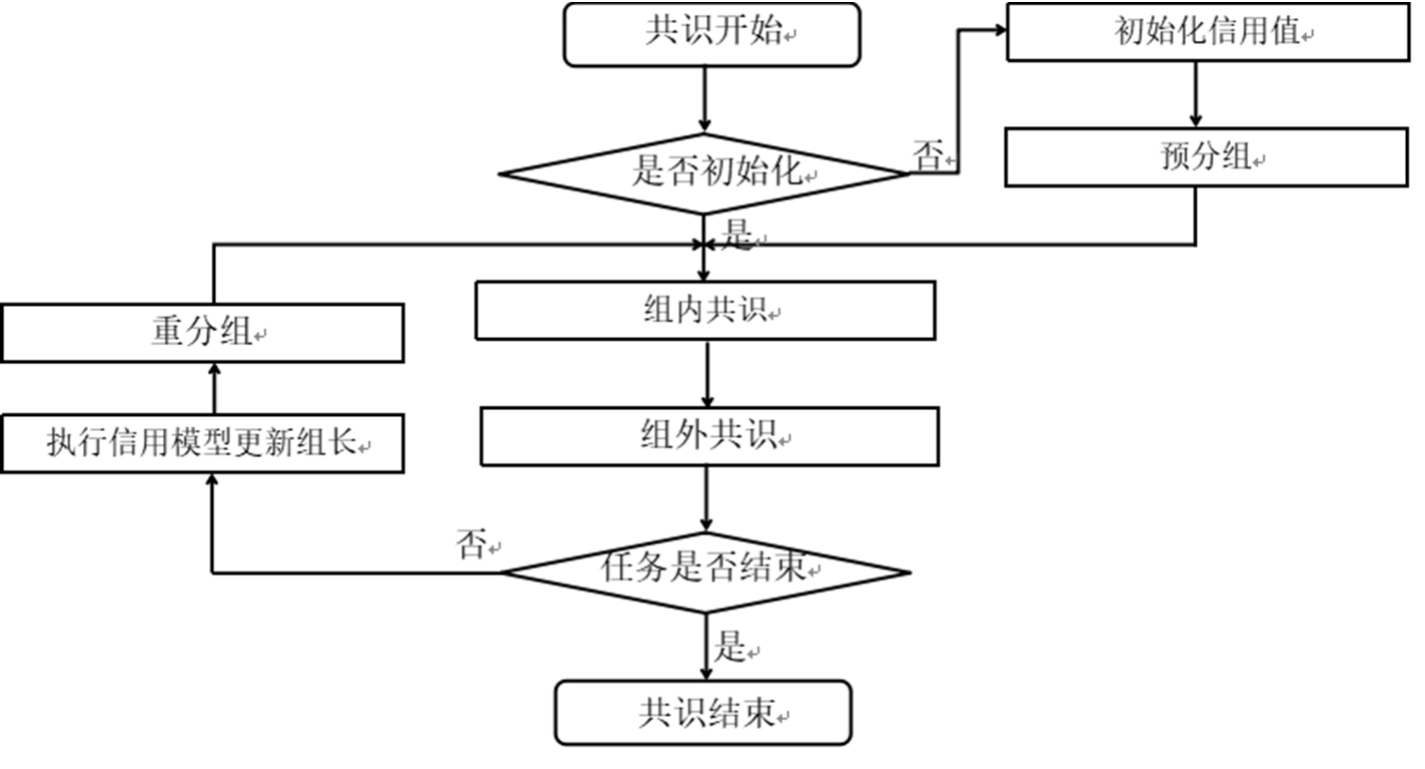


图 4-2 T-PBFT 共识流程

Figure 4-2 T-PBFT consensus process

4.2.2 分组策略

利用节点加入联盟链的身份验证机制，选取*G* 个节点作为预备管理节点，假设在整 个区块链启动前，网络上的全部节点都处于孤立状态，根据节点对预备管理节点的响应 速度作为分组依据，将节点划分为*G* 个组。具体分组步骤如下：

1）预备管理节点 *c*∈(1,2,3,…,*N*) 向周围其他节点发起分组探测信息SUBSET,*t1 ,SC* ， 其中*t1* 为时间戳，*SC* 为预备管理节点*c* 的签名；

2）节点*x*∈(1,2,3,…,*N*) 收到分组探测消息，验证消息签名是否正确，正确则向预备管 理节点发起加入分组的申请 SUBSET−REQUEST,*x,t2 ,Sx* ，其中 *t2* 为节点*x* 的时间戳， *Sx* 为本轮签名；

3）预备管理节点 *c* 检查分组列表成员是否大于*Nmax* ，若大于 *Nmax* 或者验证节点信 息不通过，发送拒绝消息，若分组内成员小于*Nmax* ，则检查节点*x* 的信息，验证通过接 收*x* 加入分组的申请并将其添加至分组成员列表*Gx* ，其中，*Nmax* 为分组内最多节点数；

4）节点*x* 若收到管理节点的拒收信息，可以向邻近的下一个预备管理节点发送加入 申请 SUBSET−REQUEST,*x*,*t2* ,*Sx* ，重复上述步骤；

5）分组结束，预备管理节点之间广播得到的分组成员列表，验证节点信息，将该信 息下发各分组内部成员，完成分组确认。分组的最终结果是形成以管理节点为中心的多 个簇，每个分组管理节点负责维护组内成员，如图 4-3 所示。注意： 当分组时间超过给 定值或有新节点加入时，需要重新启动分组机制[79]。

管理节点是组内信用值最高的节点，作为本组的委托代理节点参与全局共识。因此， 经过一轮共识后，更新节点信用值，根据节点的新信用值选择一个新的管理节点，并按 上述流程重新分组。

针对 PBFT 中节点不能动态连接的问题，T-PBFT 算法建立了节点准入与退出机制， 准入与退出机制可以使授权节点在不影响系统结构的情况下动态加入共识网络，如图 3 所示。

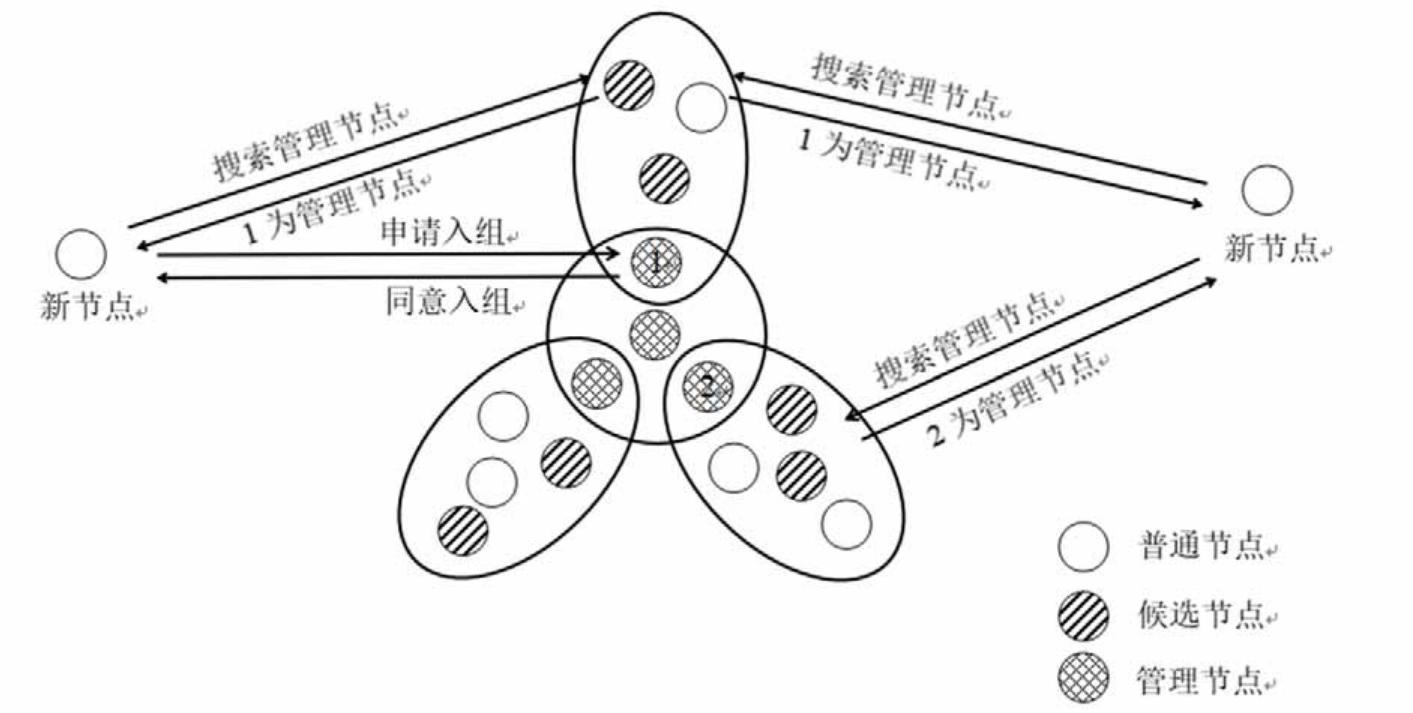


图 4-3 分组形成过程

Figure 4-3 Packet formation process

当新节点要加入网络时，首先寻找最近的管理节点，向周围节点发送搜寻请求，节 点将管理节点的信息转发给新节点并附带时间戳，对比时间戳，向先收到回复的节点的 管理节点发送入组申请，管理节点需要将新节点信息添加至组内成员列表并向新节点提 供组内其他节点的信息，新节点加入网络完成。新节点进入网络后为普通节点， 不参与

共识，只接收共识结果。

节点退出机制，若退出网络的为管理节点，首先要广播消息将身份降为候选节点， 等待新的管理节点选举成功，向管理节点报告退出；若是候选节点或普通节点退出网络， 直接向管理节点提出申请即可。

4.2.3 信用模型与投票机制

区块链分布式结构的特点，存在网络节点状态不稳定等特性，共识机制稳定运行需 要可信的节点。将网络节点划分成各分组后， 引入信用模型与投票机制作为选举参与全 局共识节点的依据。

信用模型用来计算每个节点的信用值，而信用值由共识过程中节点自身的行为决定。 为了便于计算，节点*x* 的信用值*Cx* (*t* )取值范围设置为[0，10]，初始信用值为5 ，该值越大， 节点就越可信。每个节点的信任值应该根据其历史时期的信用值进行调整， 从公式(1)可 以看出，该调整机制可以根据每轮共识不断调整区块链网络中所有节点的信用值。具体 如下，*t* 轮共识，若有新区块产生，管理节点以及与管理节点有相同投票结果的分组成 员信用值都会增加；若管理节点未参与组外共识、分组成员未参与投票或者投票结果与 共识结果不同，则其信用值就会降低，下降速率由*y* 决定(本文*y* 取0.75 )；若管理节点或 分组成员向不同的节点发送了不同的信息，则视该节点为作恶节点，将其信用值清零。

*C* (*t*+1)={[ ,*x*不(*t* ,(发，0同 (4- 1)

*x* min(*C* (*t* )+1,10) 共识集成员与管理节点有相同投票结果

lmin**|**(*Cx* (*t* )|(1+*t*+1,|,10,**|**,新区块产生

 ( *x* ( 1, ) )

表 4-1 节点状态与权重

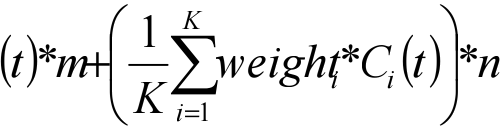
Table 4-1 Node status and weight

|  |  |  |
| --- | --- | --- |
| Cx(t) | condition | weight |
| [0,2] | malicious | 0 |
| [3,4] | abnormal | 0.3 |
| [5,7] | middle | 1.2 |
| [8,10] | excellent | 1.5 |

网络中的节点根据信用模型计算出信用值，不同的信用区间有不同的状态标识，分

别为“excellent”、“middle”、“abnormal”和“malicious”。共识节点的投票权重由 不同的状态标识决定，因此可以将权重分为0 、0.3 、1.2 和1.5 ，如表 4-1 所示。

管理节点的选举是由信用积分与投票机制最终共同决定的，节点的最终得分计算公 式如下：

*Sx* =*Cx* (4-2)

其中，*K* 为组内总节点数，*i*∈(1,2,3,…,*N*)且*x*≠*i* ，*m* 、*m* 为两个参数且*m*+*n*=1。节 点的最终得分分为基本分数和投票分数，基本分为该节点的信用值与参数*m* 的乘积，投 票分为组内其他节点的信用值与权重的乘积，本文选取了*m*=*n*=0.5 ，该投票方法能够保 证高可信的节点成为管理节点，提高系统的安全性。

视图切换协议是 PBFT 算法用来进行主节点更换的机制，T-PBFT 算法根据信用模 型与投票机制更换分组内的管理节点，信用值越高，投票节点权重越大，在管理节点更 新的过程中就有越大的概率当选为管理节点，具体步骤如下：

1）节点向分组内其他节点广播自身信用值，更新信用值列表；

2）根据信用模型投票选举管理节点，票数超过参与投票节点总数的一半有效；

3 ） 选 取 出 来 的 管 理 节 点 发 起 分 组 内 部 数 据 同 步 请 求 《DATA−REQUEST,*num*,*t3 ,SG* ,*data*，其中*num* 为区块编号，*t3* 为时间戳，*SG* 为组长签 名，*data* 为要同步的数据，分组内成员收到同步消息，检查信息是否有误，若没有异议， 更新备份数据；

4）分组成员数据同步成功，向管理节点回复同步确认消息DATA−COMMIT,*t4 ,Sx* ， 其中，*t4* 为时间戳，*Sx* 为组员签名。管理节点选举与数据同步过程如图 4-4 所示。

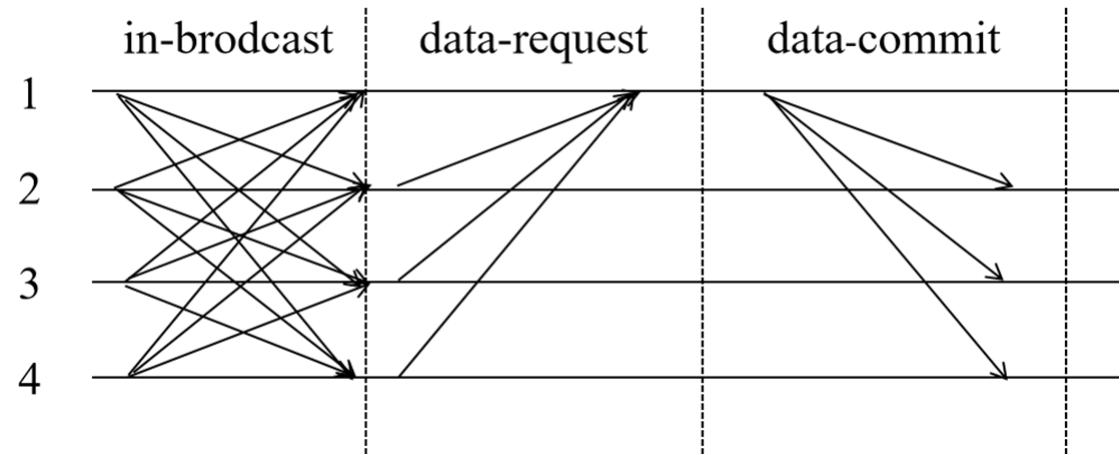


图 4-4 优化管理节点选举与数据同步

Figure 4-4 Optimized management node election and data synchronization

4.2.4 T-PBFT 算法流程

节点加入网络，随机选举预备管理节点，根据分组策略，形成不同的分组，初始化

各节点信用值，执行 T-PBFT 算法的 7 阶段一致性协议，具体如下。

1）请求阶段

客户端*c* 向各个分组管理节点发送多个交易请求REQUEST,*t,c,tx,SC* 。

2）组内准备阶段

管理节点收到消息，验证客户端消息的合法性，通过后向所有组内成员发起共识提 议 IN-PREPARE,*n*,*t*,*D*(*m*),*SG* 。

3）组内确认阶段

分 组 成 员 对 收 到 的 提 议 进 行 验 证 ， 若 无 误 则 将 对 提 议 的 回 应 IN-COMMIT,*n*,*t*,*D*(*m*),*S*x  发送给管理节点。

4）组外准备阶段

当管理节点接收到分组成员的确认消息时，会验证消息的合法性，如果确认消息合 法，代表分组内共识完成，此时管理节点代表各分组参与全局共识，向除了自己之外的 所有管理节点广播 OUT-PREPARE,*n*,*t*,*D*(*m*),*S*G  ，同时接收其他管理节点的广播消息， 进入准备阶段。

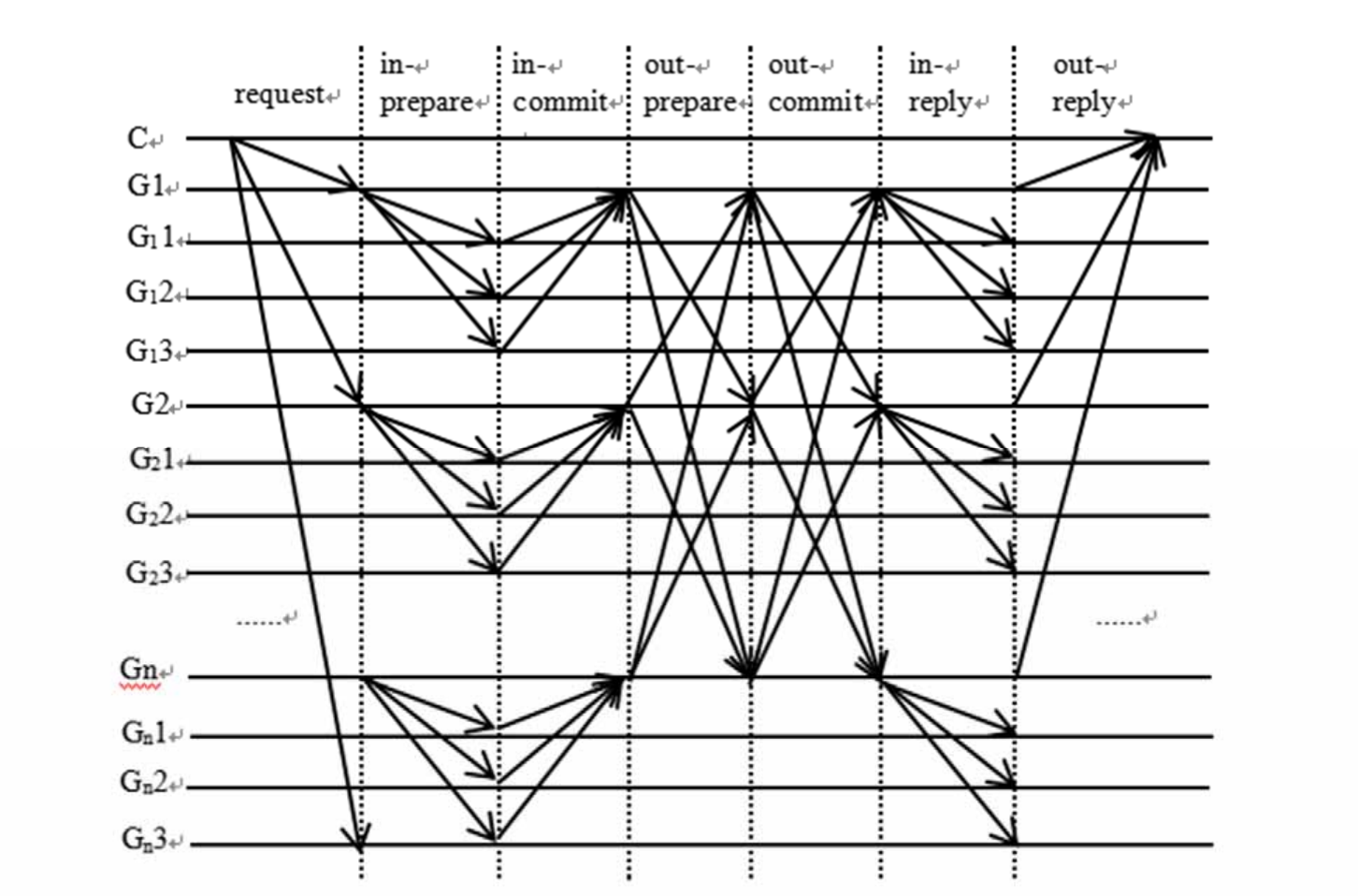


图 4-5 T-PBFT 优化一致性协议

Figure 4-5 T-PBFT optimized consistency protocol

5）组外确认阶段

各管理节点对收到的广播消息进行验证，若有异议则丢弃，若收到超过2*f* 个相同 的消息，则向其他管理节点广播 OUT-COMMIT ,*n*,*t*,*D*(*m*),*S*G  。

6）组内回复阶段

各管理节点对收到的确认消息进行验证，收到超过2*f* 个验证通过的消息，则回复

分组内各成员 IN-REPLY,*n*,*t*,*D*(*m*),*S*G  。

7）组外回复阶段

管理节点最终回复客户端 OUT-REPLY,*n*,*t*,*D*(*m*),*S*o  ，共识达成。

其中，*t* 为时间戳，*c* 是客户端编号，*tx* 为具体交易，*SC* 为客户端签名，*n* 表示区块 编号，*m* 表示需要共识的信息，*D(m)*为信息的摘要。T-PBFT 优化一致性协议如图 4-5 所示。

共识结束，计算各节点信用值，组内重新选举管理节点。若分组时间超过给定值或 新节点加入等，则重启分组，否则重复上述操作，直至全部事务结束[79]。

4.3 实验验证

实验基于 Java 编程语言模拟实现了一个区块链系统，操作系统为 Windows 10，CPU 为 AMDR7 5800H，内存为 16GB。在该系统中对本文提出的 T-PBFT 算法进行验证，分 别对不同数量的节点从吞吐量、共识延迟、通信开销、安全四个方面进行评估。重复试 验 1000 次，每次发送请求消息 200 条，取 1000 次的平均值作为测试结果。具体仿真参 数如表 4-2 所示。

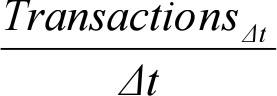
表 4-2 仿真参数

Table 4-2 Simulation parameters

|  |  |
| --- | --- |
| 名称 | 数值 |
| 客户端发送请求数量(条/次) | 200 |
| 总节点数量/个 | 30-800 |
| 拜占庭节点占比 | 10% 、20% |
| 分组数 | 30-50 |
| 信用值区间 | [0,10] |
| 初始化信用值 | 5 |

4.3.1 T-PBFT 算法吞吐量测试

在区块链系统中，吞吐量 TPS 指的是在单位时间内完成交易的数量。高吞吐量的系 统可以在有限时间内处理更多的交易事务。计算公式如下：

*TPS*= (4-3)

其中*Transaction*sΔt 表示 *Δt* 时间内完成交易的数量，*Δt* 表示交易发出到交易上链的 时间间隔。

1）实验通过设定不同数量的节点，计算一秒钟内完成的交易数量，最终的结果如 图 4-6 所示。

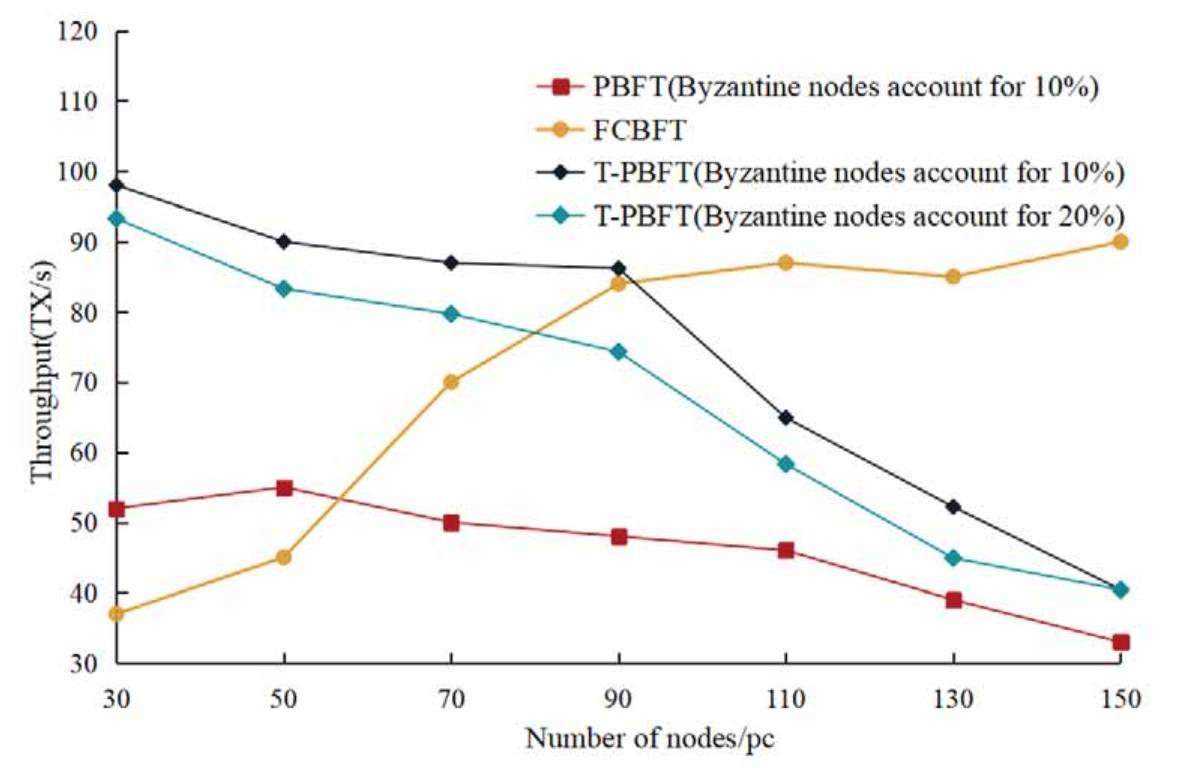


图 4-6 PBFT 、FCBFT 和 T-PBFT 吞吐量对比

Figure 4-6 Comparison of PBFT, FCBFT and T-PBFT throughput

实验验证 PBFT 、FCBFT[80]与 T-PBFT 算法(网络中分别有 10% 、20%数量拜占庭节 点)不同数量节点下，每秒能够完成的交易数量。可以看出，PBFT 和 T-PBFT 算法网络 中的共识节点数与拜占庭节点数都相同时，T-PBFT 的吞吐量相比 PBFT 更高；T-PBFT 算法参与共识的节点数量不变，提高拜占庭节点占比，吞吐量仍然能保持稳定状态。随 着共识节点的增加，FCBFT 算法吞吐量增加，PBFT 与 T-PBFT 算法的吞吐量整体呈现 下降趋势。

2）为了更详细地测试 T-PBFT 算法的性能，进一步增加节点的数量，并测试 T-PBFT 算法在不同分组数量下的吞吐量，如图 4-7 所示，分别选取 200、300、400、500、600 、 700 、800 个节点，设置分组数目为 30、40 、50。可以看出， 无论 T-PBFT 算法的分组数 目为多少，其吞吐量皆优于 PBFT，且在一定范围内随着分组数目的减少吞吐量在逐渐 增加，分组数为 30 时，吞吐量明显优于设置分组数目为 50 的情形。

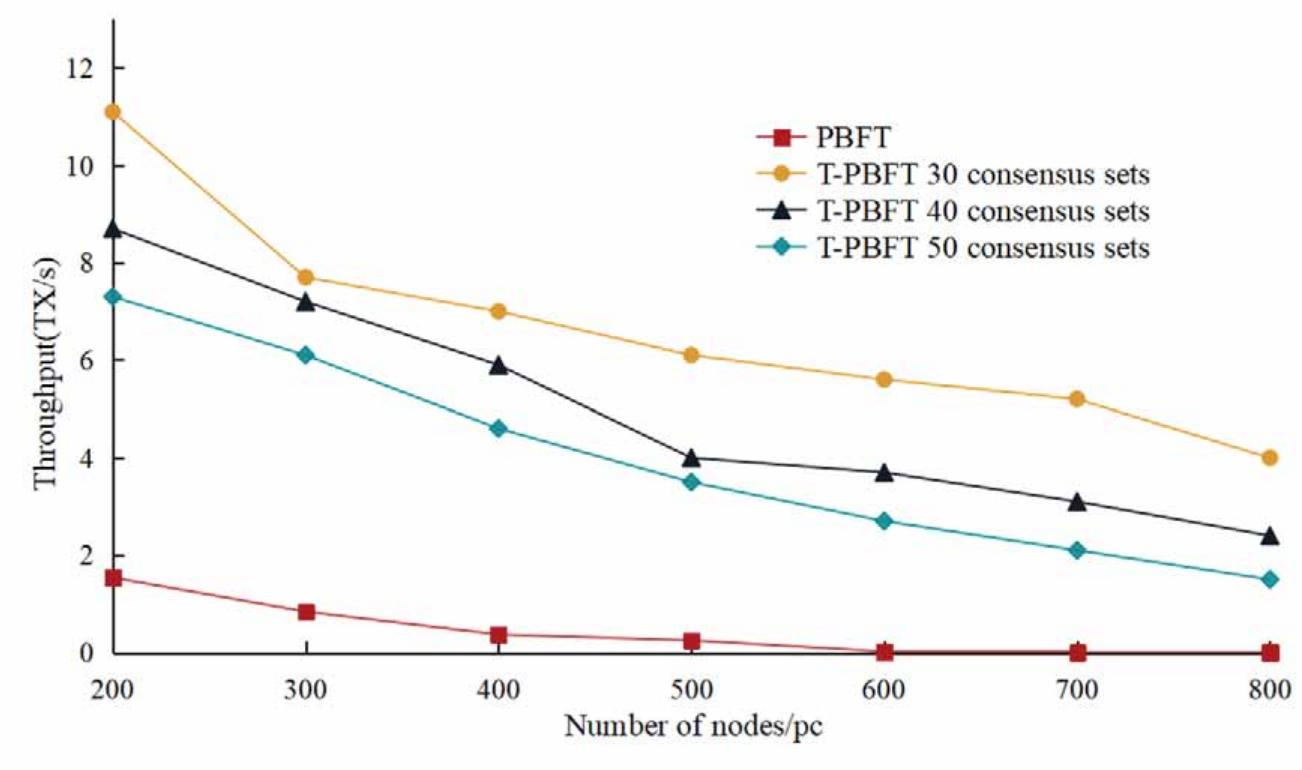


图 4-7 PBFT 、T-PBFT 吞吐量对比

Figure 4-7 Comparison of PBFT and T-PBFT throughput

4.3.2 T-PBFT 算法共识延迟测试

共识时延表示从客户端发送交易请求到客户端完成交易确认所需的时间。低延迟表 明，共识算法执行时间较短，区块链不易发生分叉，系统的安全性及运行效率较高。延 迟公式表示如下：

*Delayconsensus*=*TC* −*TR* (4-4)

其中，*TC* 表示交易确认时间，*TR* 表示交易生成时间。在相同的条件下，PBFT、FCBFT 和 T-PBFT 三种算法的时延如图 4-8 所示。

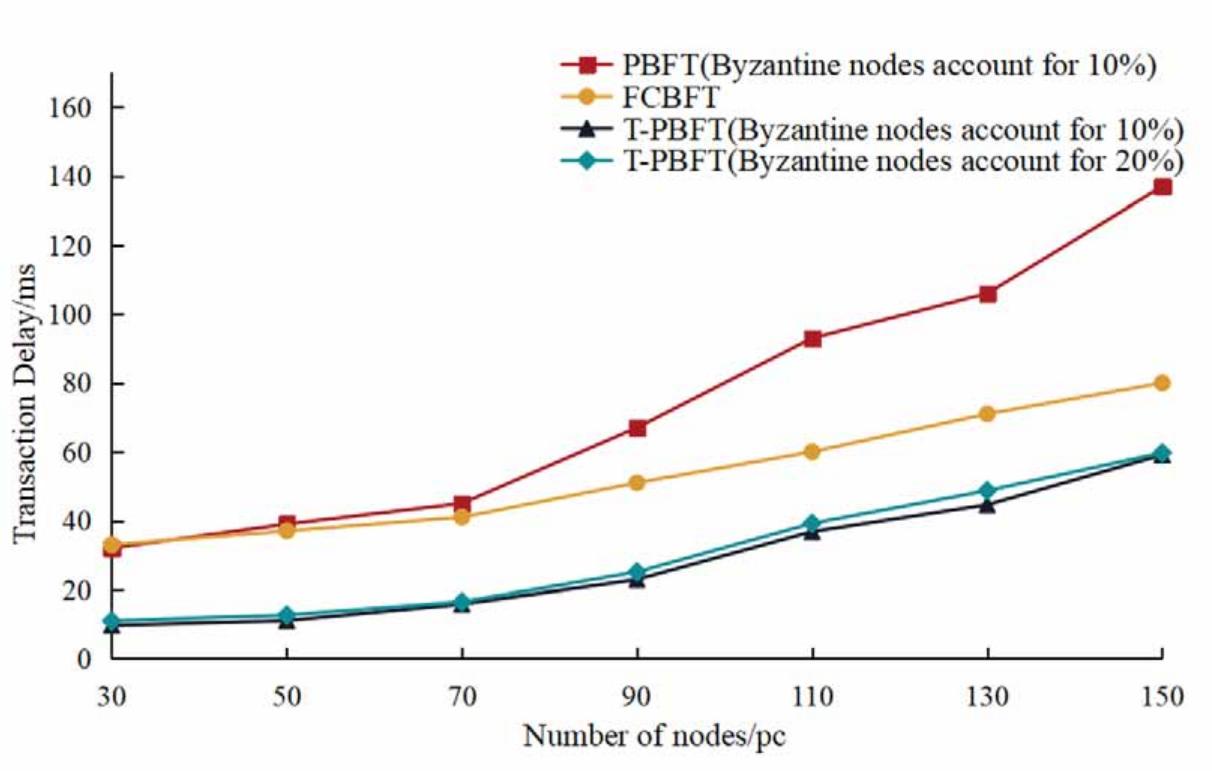


图 4-8 PBFT 、FCBFT 和 T-PBFT 交易时延对比

Figure 4-8 Comparison of transaction delay among PBFT, FCBFT and T-PBFT

可以看出，共识节点数量相同，T-PBFT 算法时延明显优于 PBFT 和 FCBFT 算法， 且随着节点的增加，PBFT 算法的共识时延增长的幅度比 T-PBFT 算法大很多，特别是 当网络节点个数超过 70 时，PBFT 的延迟急剧增加，而 T-PBFT 算法仍然比较稳定。与 此同时，拜占庭节点占比 10%或 20% ，T-PBFT 算法的交易时延无明显变化，因此，能 很好的对抗恶意节点对溯源系统的影响。

4.3.3 T-PBFT 算法通信次数测试

通信开销是指网络各节点在共识过程中产生的通信量。

PBFT 共识过程的三个主要阶段，分别是预准备（pre-prepare）、准备（prepare） 和确认（commit）阶段，对于预准备阶段，主节点广播消息给所有的从节点，通信次 数为*N*−1（其中， *N* 为节点数量）；对于准备阶段，节点向除它们自己以外的所有节 点发送验证消息，通信次数为(*N*−1)2 ；确认阶段，各节点向其他节点广播确认消息， 通信次数为*N*\*(*N*−1)。因此，PBFT 算法的总通信次数为：

*T1* =*N*−1+(*N*−1)2 +*N*\*(*N*−1)=2*N*\*(*N*−1) (4-5)

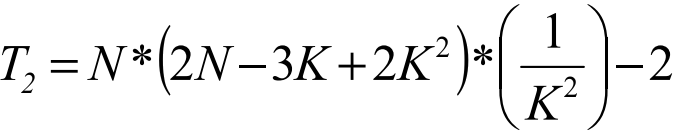
改进的 T-PBFT 算法在节点共识的过程中增加了分组阶段以及节点信用值的计算， 在 T-PBFT 算法中客户端向管理节点发起提案，通信次数为*G* (其中，*G* 为分组个数)； 组内准备阶段，管理节点广播消息给分组内部成员，通信次数为[*N*−1*G*−1]\**G* ；组内确认阶 段，各分组成员向管理节点发送消息确认，通信次数为[*N*−1*G*−1]\**G* ；组外准备阶段，管理 节点向除自身以外的其他管理节点广播消息，通信次数为(*G*−1)\**G* ；组外确认阶段，各 管理节点对收到的消息进行验证，向其他管理节点广播，通信次数为(*G*−1)\**G* 。T-PBFT 算法的总通信次数为：



= (2*G* − 3)\**G* + 2(*N* −1)

(4-6)

假设*G*=*NK* ，*K* 表示分组内部成员数，为大于 3 的任意常数，上式化简为：

 (4-7)

当*N*>12 时，*T*2 >*T*1 ，因此改进后的通信时间更少。

图 4-9 为 PBFT 和 T-PBFT 的通信量相对增长率，从图中可以看出，随着节点数量 的增加，通信量相对增长率从约 81.2%上升到约95.0%，且相对增长率将继续上升。当

节点数超过 70 个后，其增长趋势明显加快。

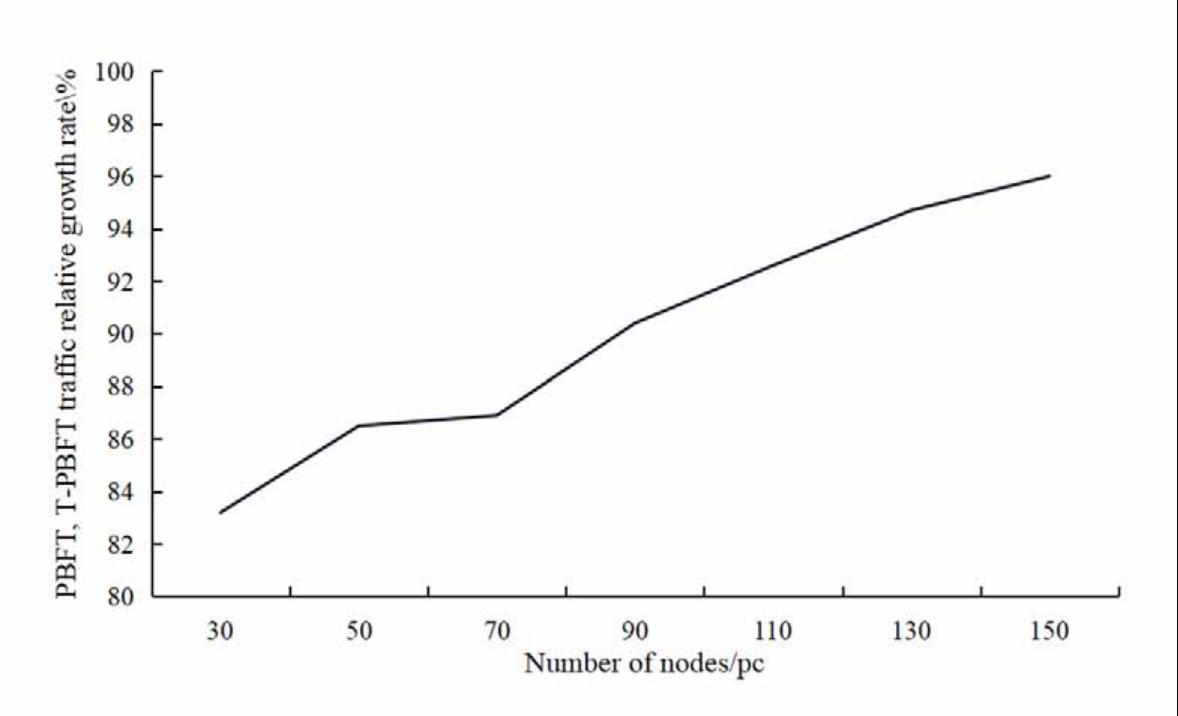


图 4-9 PBFT 、T-PBFT 算法通信量相对增加率的比较

Figure 4-9 Comparison of relative increase rate of traffic between PBFT and T-PBFT algorithms

4.3.4 T-PBFT 算法安全测试

安全性是区块链系统中的一个重要属性，恶意节点是导致共识失败的一个重要原因。 为了评估 T-PBFT 算法的安全性，分别测试了共识节点的信用值变化与容错性。结果表 明提出的分组策略与信用投票模型能很大程度提高主节点的可靠性、增加系统容忍拜占 庭节点的个数。

1）共识节点信用值

根据共识节点的行为检测其信用值的变化，能够反应该节点的可靠性，也能够检测 系统的安全性。

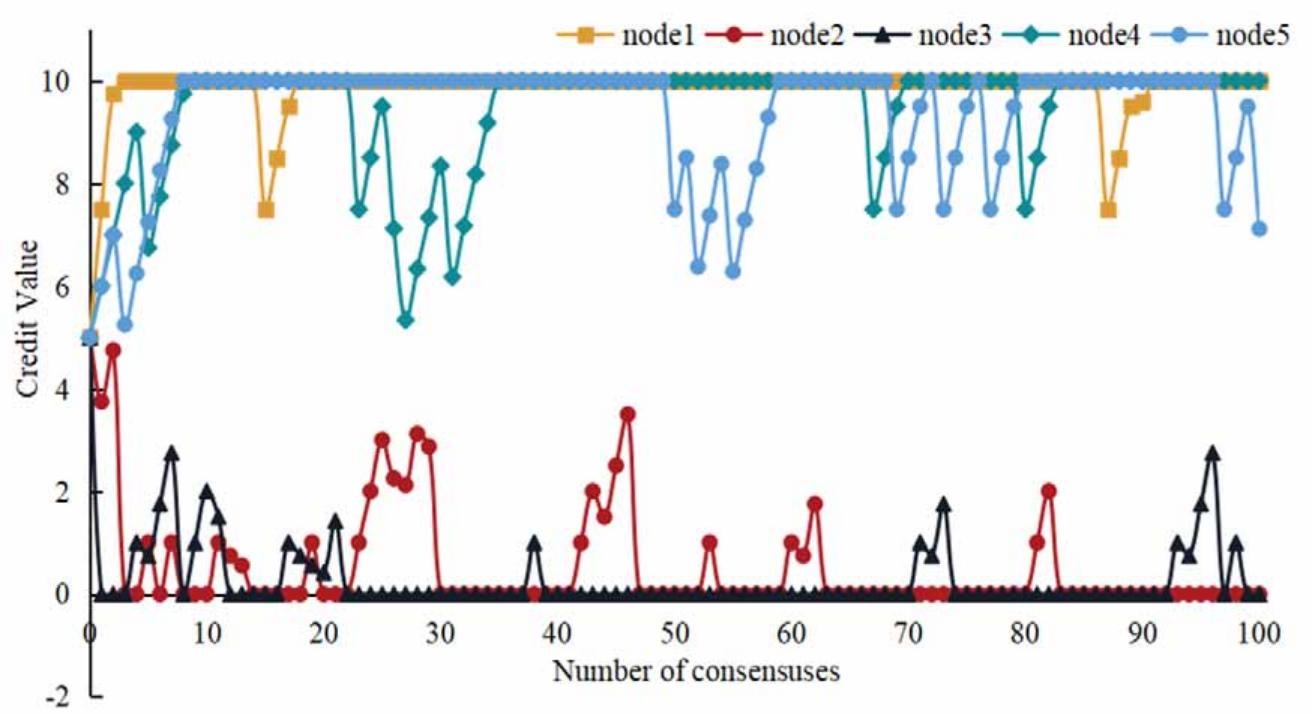


图 4-10 节点信用值变化

Figure 4-10 Node credit value change

根据共识情况，查看不同节点 node1 到 node5 的信用值变化，设置 node2 与 node3

为恶意节点，每个节点初始信用值为 5，第一轮共识过程，node2 节点未参与投票，信用 值降为 3.75；node3 向不同的节点发送了不同的信息，信用值降为 0；node1 因成功出块， 获得信用度奖励，信用值为 7.5；其余节点均正常节点，共同达成共识，信用度均增加为 6。图 4-10 为 100 轮共识节点 node1 到 node5 的信用值变化。

从中可以看出，node1 节点的信用值波动较少，node4 与 node5 的信用值在 9 左右 波动，而 node2 与 node3 因为发送恶意信息，其信用值在 1 左右。因此， 共识过程中表 现良好的节点都会给予相应良好的信用值，恶意节点的信用值也会保持较低水平。

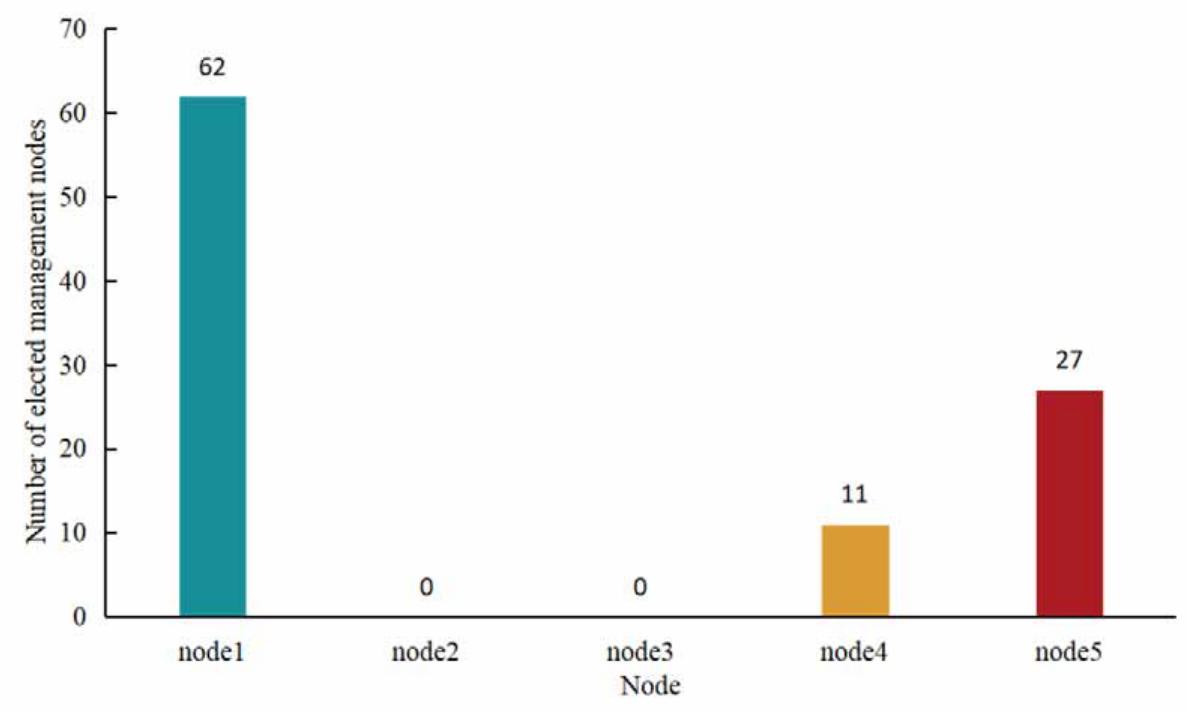


图 4-11 节点当选管理节点次数统计

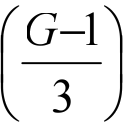
Figure 4-11 Statistics on the number of nodes elected to the management node

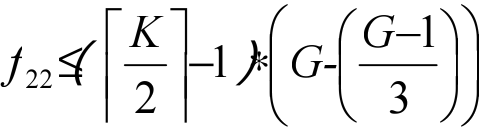
图 4-11 表示，前 100 次共识，节点 node1 到 node5 当选为管理节点的次数，从图中 可以看出，信用值较好的节点 node1 当选了 39 次管理节点，高于其他节点，信用值较 差的节点 node2 和节点 node3，均未当选管理节点，node4 与 node5 信用值相差不大，分 别当选管理节点 29 次与32 次。通过选举信用值较高的节点作为管理节点， 有助于降低 恶意节点获得记账权的风险，进而有效地维护区块链系统的安全性和可靠性。

2）容错性

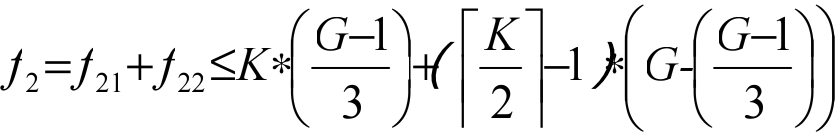
容错性是指区块链系统中最多能容纳的拜占庭节点数量。联盟链有严格的身份验证 机制，但仍然不能阻止恶意节点伪装成正常节点进入联盟链。

PBFT 算法最大容错为*f*1 ≤(*N*−1) 3 ，T-PBFT 算法将节点分配到不同的分组，最多能容 纳的拜占庭节点数为 13 组内节点全为拜占庭节点 *f*21 与 2 3 的组内拜占庭节点占比 49%*f*22 之和。

*f* 21 ≤*K*\* (4-8)

 (4-9)

系统容错性达到：



(4- 10)

|  |  |
| --- | --- |
| 化简整理： |  |
|  | (4- 11) |

其中*N*(*N*≥12) 为总节点数，*K*(*K* ≥3) 为组内节点数，*G*(*G*≥4) 为分组个数。

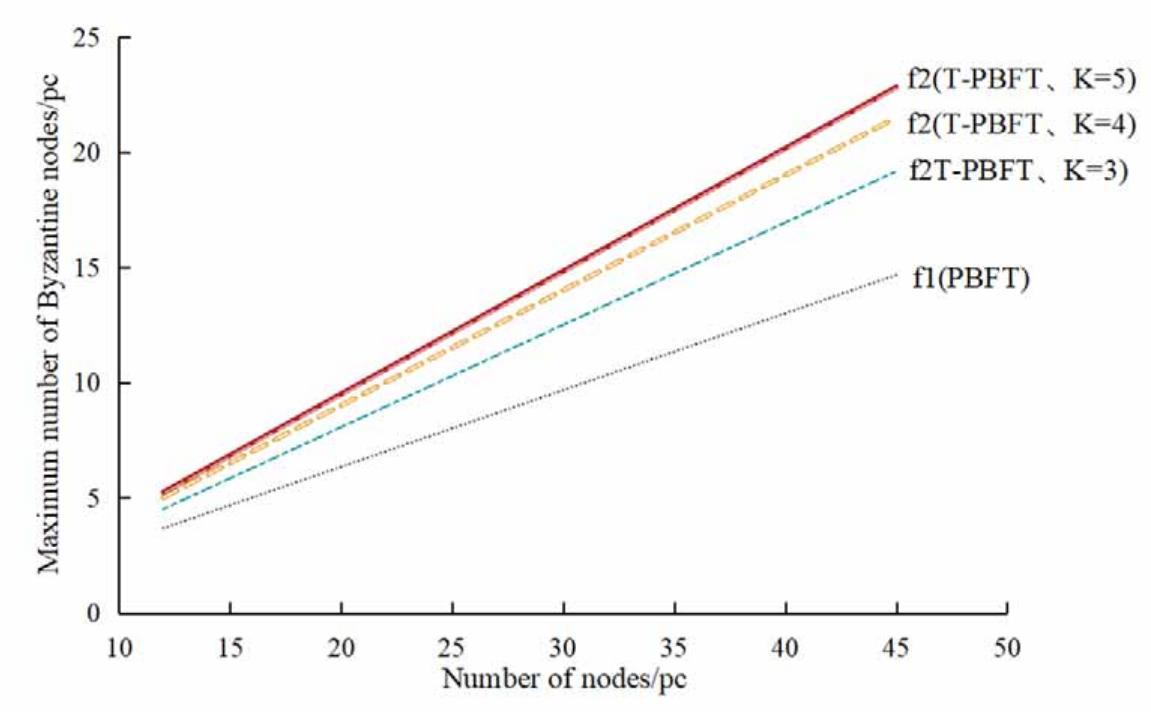


图 4-12 T-PBFT 、PBFT 最多容纳拜占庭节点数

Figure 4-12 The maximum number of Byzantine nodes in T-PBFT and PBFT

T-PBFT 算法与 PBFT 算法最多能容纳的拜占庭节点数如图 4-12 所示，可以看出 T- PBFT 算法的容错性均优于 PBFT 算法。网络中节点数较少时，两算法的容错性相差无 几，随着节点数的增加，相较于 PBFT 算法，T-PBFT 算法所能容纳的拜占庭节点数量增 长速率更快，并且随着*K* 值(组内节点个数)的增加，网络能容忍的拜占庭节点也越来越 多，因此，可以说明 T-PBFT 算法的容错性优于 PBFT 算法。

4.4 本章小结

本章简要介绍了 PBFT 算法，并针对 PBFT 算法支持的网络规模有限、通信开销大、 系统消耗高等弊端，结合基于区块链的农产品溯源的特征，提出了一种基于分组和信用 投票的改进算法 T-PBFT，将大规模网络节点划分为不同的分组，进行分组共识并基于 信用值与投票机制选择管理节点，降低管理节点成为拜占庭节点的概率，提高系统的效 率和安全性。最后通过实验验证，T-PBFT 可以减少通信开销与交易延迟，提升吞吐量

与安全性，增加溯源规模。

第 5 章 农产品溯源系统的应用实现

5.1 系统角色需求分析

本文旨在构建一个基于区块链的农产品溯源系统，市面上食用农产品种类繁多，其 溯源环节也不尽相同，本文选择以有机大米溯源为例分析基于区块链的农产品溯源需求。

基于区块链的有机大米追溯系统是一个面向多环节、多参与者的综合系统。该系统 主要为三部分人群服务：供应链参与人员(农户、存储仓、加工厂、零售商、运输商) 、 消费者以及监管部门、区块链系统管理人员。系统角色用例图如图 5-1 所示。

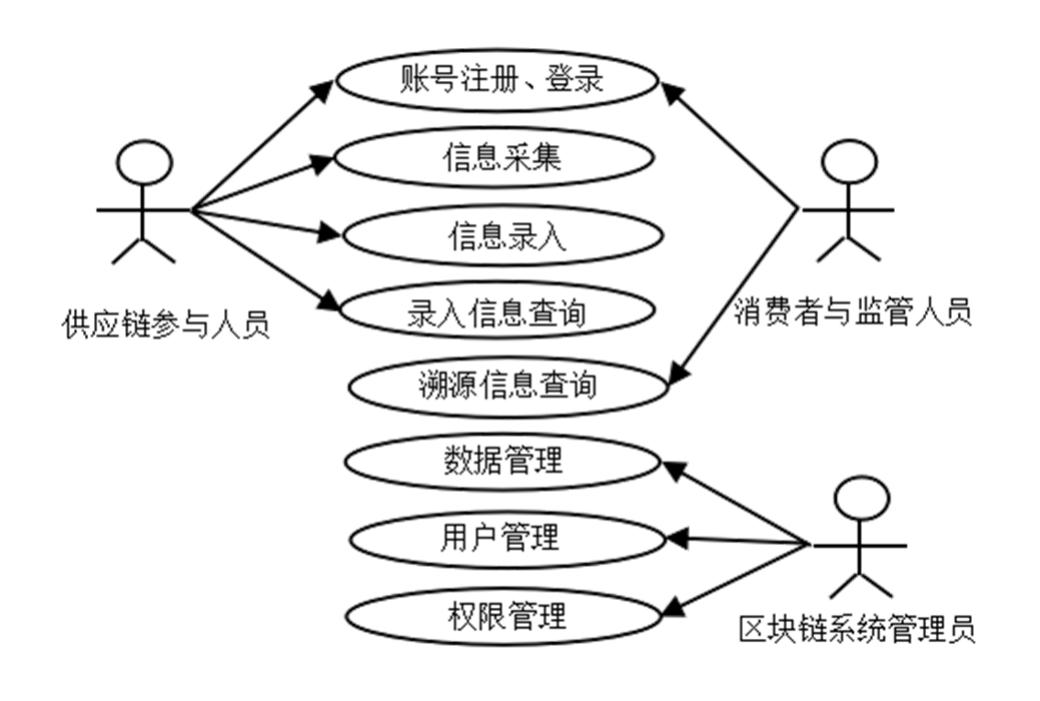


图 5-1 有机大米溯源系统用例图

Fig. 5-1 Use case diagram of organic rice traceability system

1）供应链参与人员

供应链参与人员包括农户、存储仓、加工厂、零售商、运输商五类， 作为有机大米 追溯系统的主要用户，需要先进行注册登录，经过系统管理人员审核来完成身份的认证。 参与人员具有信息采集、录入等功能， 通过智能合约的交互完成供应链上下游的信息存 储，实现追溯环节信息的全覆盖。

2）消费者以及监管部门

消费者以及监管部门作为溯源体系的最后一个环节，起着至关重要的作用，决定着 有机大米的质量是否合格。进入追溯系统， 根据自身需求选择是否注册，若只是查询有 机大米相关追溯信息，可以选择游客身份，输入有机大米包装上的溯源码，就可以直接 查询到该产品从种植存储到生产加工运输销售等一系列信息。一旦监管部门发现产品异 常，可以根据上下游的信息，追踪和召回同批次的产品，同时对问题进行排查，确认异 常起源，给与相应惩罚措施。

3）区块链系统管理人员

系统管理人员也是系统的重要用户之一，有数据管理、用户管理以及权限管理三大 主要功能。通过审查供应链参与人员的用户注册情况， 进行角色及权限分配，确保信息 的真实性。

5.2 系统功能分析

基于区块链的农产品溯源系统被划分为多个模块，包括用户管理、数据上传、信息 查询和监管等模块，具体见图 5-2。接下来将依次介绍各主要功能模块。

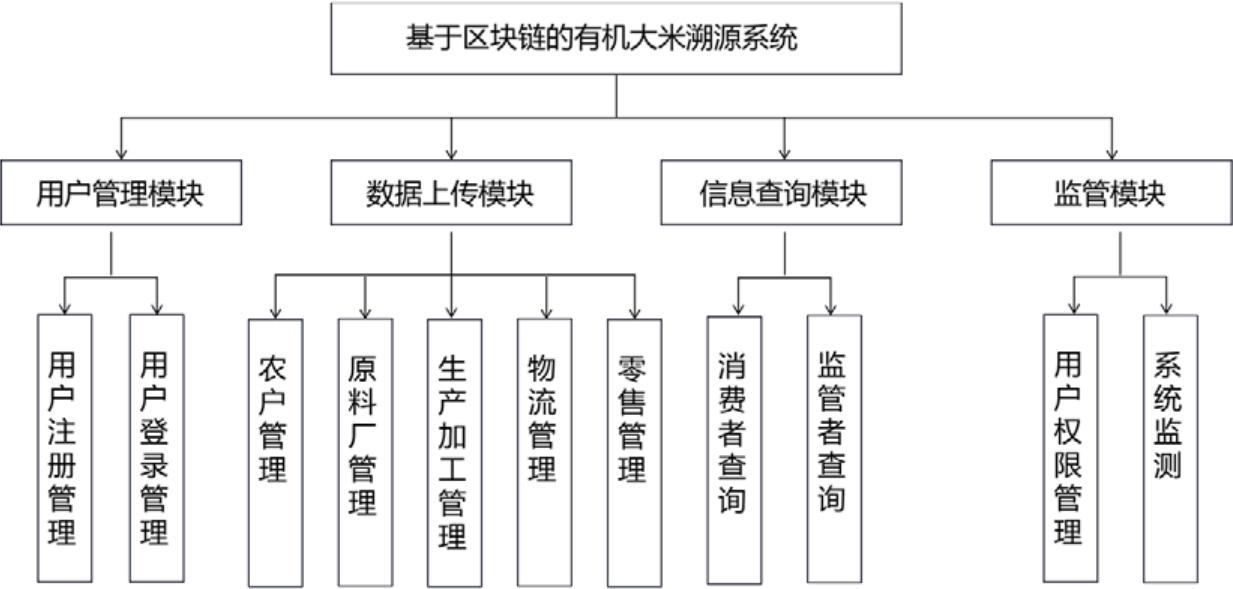


图 5-2 系统功能模块

Figure 5-2 System function module

1）用户管理模块

用户管理模块主要涉及用户的注册、登录以及权限管理等功能。供应链所有用户（包 括农户、存储仓、加工厂、零售商、运输商以及区块链管理人员） 在第一次使用区块链 溯源系统时，需要输入用户姓名、用户名、密码、手机号等信息进行注册登录， 用户根 据不同的身份进行登录，不同的身份有不同的区块链操作权限，由管理员事先设置，为 了保证可靠性，上述数据需要得到区块链网络上所有节点的验证和共识。一旦达成共识， 系统将生成用户的区块链地址，并将用户的个人信息及区块链地址存储在本地进行数据 备份。

2）数据上传模块

每当有新的农产品信息录入系统时，数据上传模块将使用共识机制和智能合约对供 应链参与者（包括农户、存储仓、加工厂、零售商、运输商） 所提交的农产品信息进行 上链操作，并在成功上链后将数据保存在本地。

3）信息查询模块

当消费者输入溯源码发起查询后，系统会在根据输入的溯源码进行查找，生成农产

品溯源信息，查看到该农产品种植、存储、加工、运输、销售等全过程信息。

4）监管模块

区块链系统管理员对供应链上的参与人员进行权限管理和身份认证，对消费者投诉 的信息进行核实并做相应的处理。

5.3 系统业务流程设计

在开发 Fabric 溯源系统之前，根据系统的需求，把项目中可能涉及的参与方列出来， Fabric 的参与成员需要通过 Membership Service Provider（MSP）来完成注册，并实现对 身份的验证，授权和管理。供应链中不同身份的用户会有不同的访问权限和读写权限。 消费者有权查询溯源信息，但无权修改信息。监管部门和执法部门具备系统的最高权限， 负责监控各环节的有序、稳定运行。

Hyperledger Fabric 体系结构的核心是 Peer 和 orders service。将启动的 Peer 加入 channel（通道）中，使其处于同一个区块链网络下，设计完成的智能合约部署到对应的 Peer 节点中。

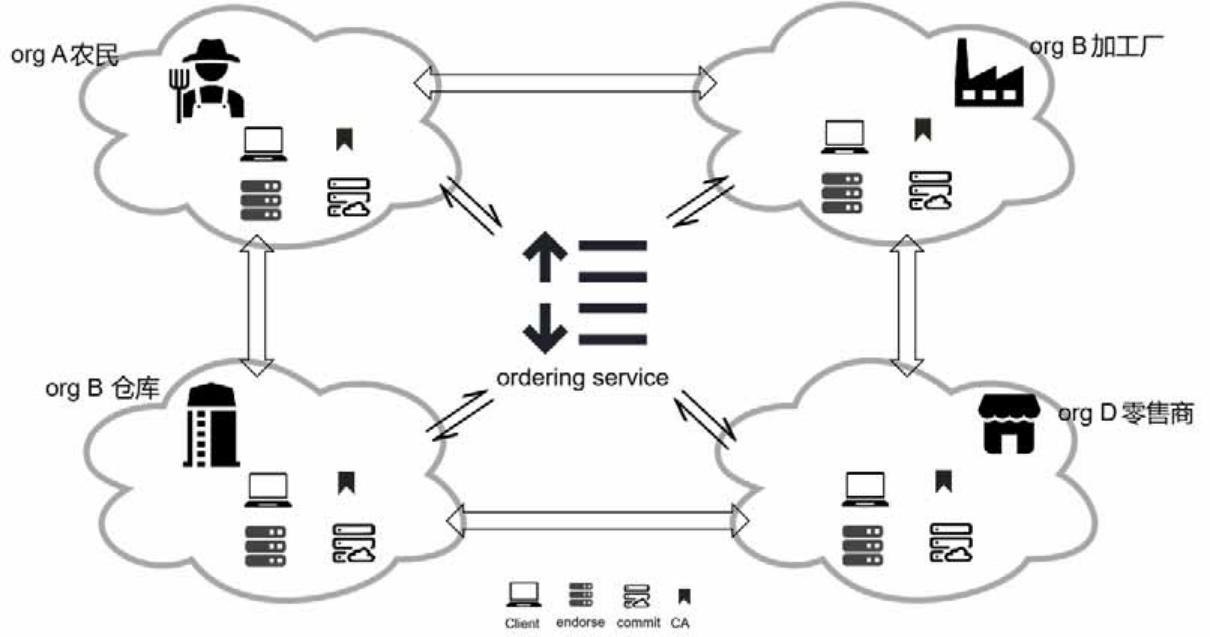


图 5-3 有机大米溯源系统业务场景图

Figure 5-3 Business scenario diagram of organic rice traceability system

图 5-3 为溯源系统业务场景图，图中列出了有机大米溯源过程中关键的几个节点： 农民、存储仓、加工厂、零售商。每个组织有自己的 CA 机构、背书节点和提交交易节 点，具体流程如图 5-4 所示。

1）用户通过客户端提交事务，通过加密签名形成区块，广播给提交交易节点验证上 链；

2）用户经过 CA 认证后，通过客户端应用程序发送交易提议；

3）交易提议是一个调用带有特定参数的智能合约的请求，由背书策略决定该请求 被提交给哪个背书节点，背书节点收到请求后，在节点模拟执行交易，但是不会更新

WorldState。需要说明的是， 每个智能合约都有一个背书政策，说明哪些组织或者节点必 须签署/检查该提议。客户端应用程序需要收集到满足智能合约的背书政策的背书。

4）背书节点将背书结果（签名与仿真产生的读写集）发送回客户端应用程序，作为 对提交的交易提议的响应。

5）当客户端应用程序收到足够的背书响应时，在事务消息中组装并将其发送到排 序节点。

6）排序节点使用可插入的共识协议来计算和建立每个通道中所有提交事务的执行 顺序，按特定顺序将多个交易打包成块，将形成的区块广播给提交节点。

7）提交节点根据智能合约的“背书策略”检查背书是否有效，并验证读写集版本号 是否正确。如果背书无效（例如签名不够）或读写集版本号错误，则该交易为无效。如 果没有问题，提交节点将提议记入账本更新 WorldState。

8）最后，提交节点将发送一个事件给发送交易提议的客户端应用程序，告诉它提议 是否上链成功。

成功上链的事务，同时也可以满足监管部门对食品质量的监督，一旦发现食品安全 问题，通过追溯系统可以找到具体环节，快速准确地定位相关责任人并采取一些行动对 欺诈的参与者实施惩罚，或采取替代和纠正措施，同时产品可以实现快速召回。

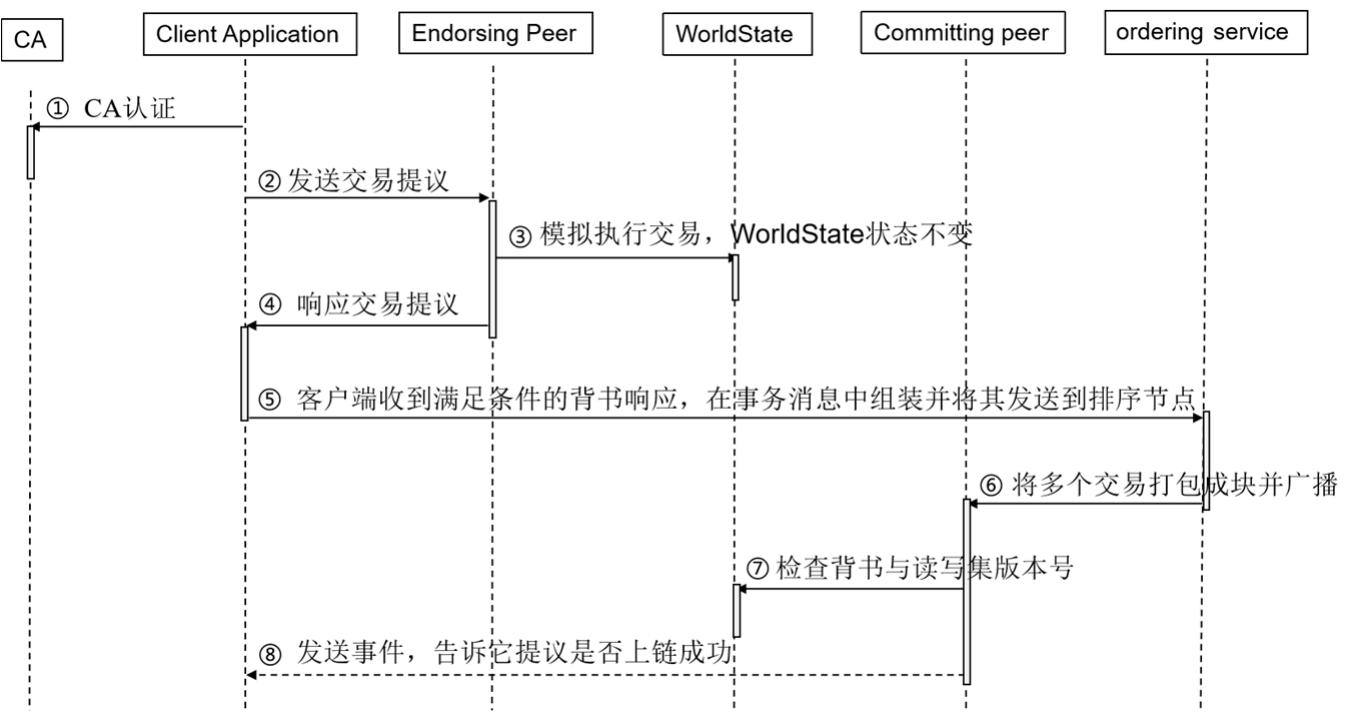


图 5-4 有机大米供应链中的事务流程图

Figure 5-4 Transaction flow chart in organic rice supply chain

在确认组织与其职责后，接下来要解决的问题就是各组织之间的通信。HyperLedger Fabric 提供了 channel（通道）这一概念，它允许一组参与者创建一个单独的共同维护的 交易账本，它是两个或多个特定网络成员之间通信的私有“子网”，用于私人和机密交 易，对于其他竞争对手来说，这是一个非常重要的选择。例如， 存储仓库可能会向某些 加工厂提供特别价格，而其他加工厂无法享受该优惠价格。但如果这些加工厂位于同一 通道上，那么它们以及同一通道的其他参与者都将了解到这个价格信息，可以看到账本

上的任意信息。因此满足了不同业务场景下的不同的用户访问不同数据的基本要求。此 外，一个参与者也可以接入多个通道，如图 5-5 所示，图中仓库订阅通道 2 和通道 3 ， 维护灰色和褐色账本；农民订阅通道 1 、2 、3 并维护灰色、褐色、黑色账本。在这个例 子中，农民订阅了所有通道，每个通道都有一个相关的账本。一般来说，不涉及所有 peer 节点的账本为子账本，另一种是系统账本，即全账本。

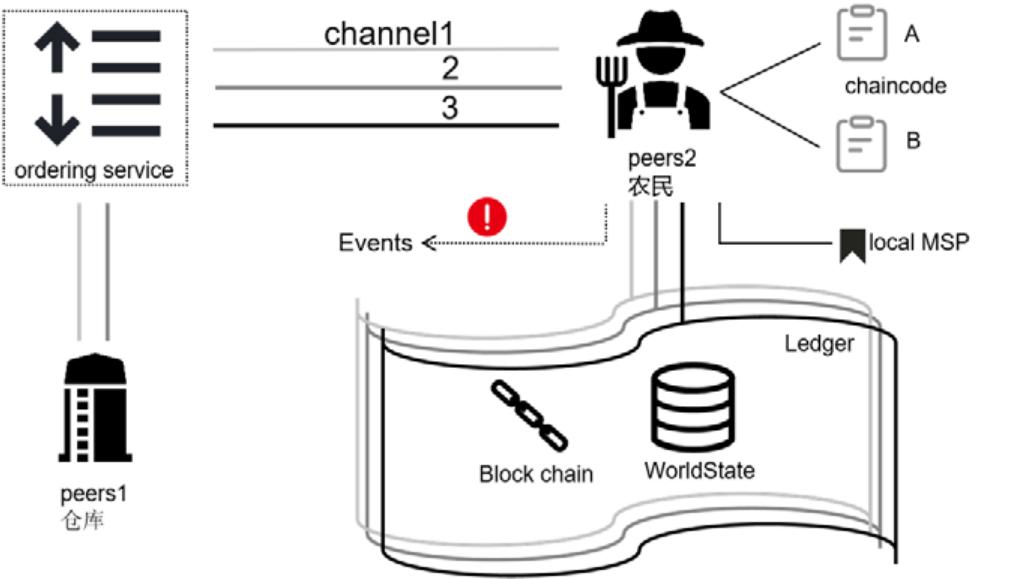


图 5-5 节点与通道关系图

Figure 5-5 Node-Channel relationship diagram

5.4 系统架构设计

基于区块链技术的农产品溯源系统，根据业务内容进行了模块化分类，主要分为 5 层：数据采集层、存储层、合约层、共识层、应用层，如图 5-6 所示。

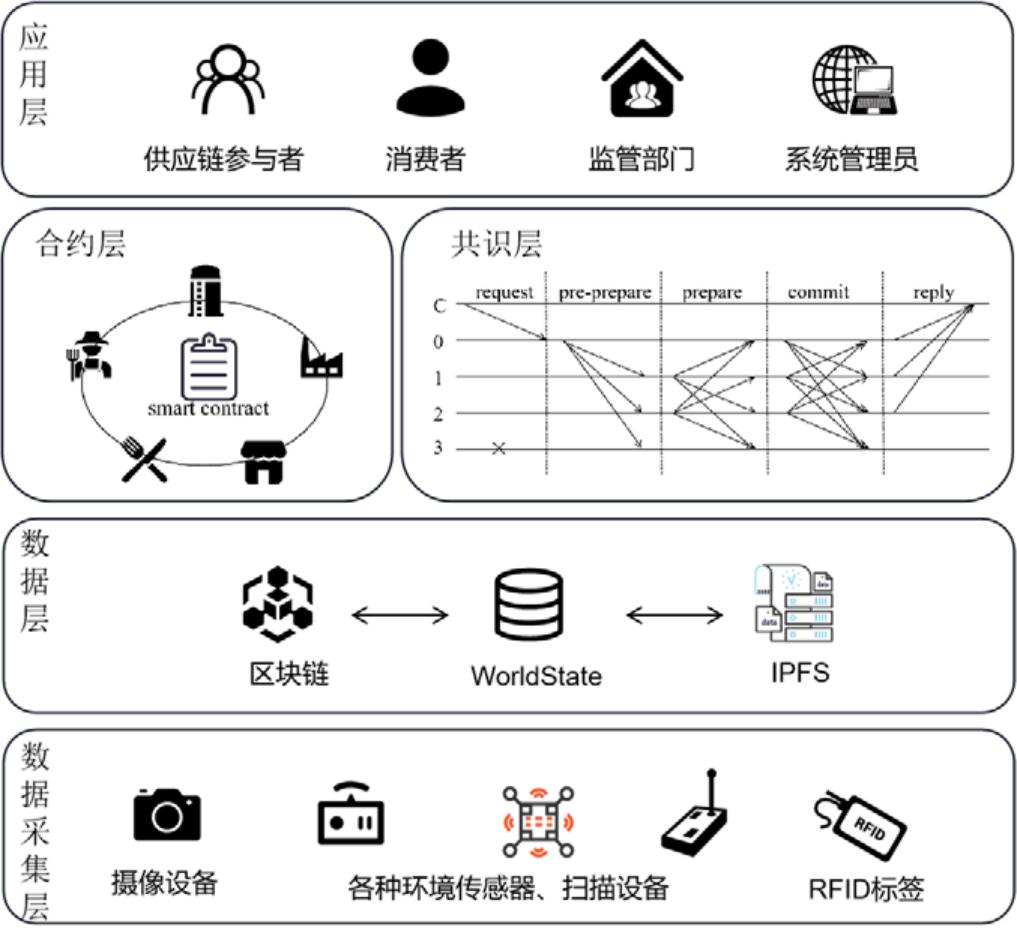


图 5-6 有机大米供应链系统框架

Figure 5-6 System framework of organic rice supply chain

最底层是数据采集层，利用 RFID、各种传感器（湿度传感器、温度传感器、声音传 感器、压力传感器等） 、GPS 等采集有机大米供应链上相关信息，内容包括前面所讲的 各实体的需求列表，都是与农产品质量安全相关的重要信息。

存储层存储数据采集层收集到的信息，采用链上链下双存储模式，由区块链和 IPFS 构成，公开数据直接上传 IPFS 和区块链，隐私数据完整的存储在链下数据库IPFS，经 过加密后再上传区块链，可以有效保证数据的安全。

共识层利用 T-PBFT 共识机制，对交易信息进行验证和确认，以确保各节点信息一 致，不会被随意篡改。

合约层是由 Go 语言编写实现的，主要负责数据存储、检索、过滤和权限控制等逻 辑。合约由主集群的联盟管理方发布， 并在获得其他供应链节点的授权背书后部署到区 块链网络中。将交易规则、国家法律条例等内容编译部署至区块链中， 在特定情景下可 以自动触发并执行智能合约，实现自动化，提高了交易的效率。

应用层采用 B/S 架构，供应链上的参与者负责信息的录入，监管部门和消费者可以 通过该系统查询农产品信息。

5.5 系统功能实现

5.5.1 环境配置

区块链系统基于 Linux 系统环境，构建了一个基于多个 Docker 容器的 Hyperledger Fabric 分布式网络环境。

shell 脚本主要用于构建网络，智能合约采用 Go 语言实现，并通过相关的依赖 NodeSDK 开发，实现接口的资源调用，Shell 脚本用于构建网络、部署节点等操作，采 用 Go 语言实现智能合约，NodeSDK 是一个用于开发和管理 Hyperledger Fabric 区块链 网络的软件开发工具包，使用 NodeSDK 来实现与区块链网络的交互和通信。应用系统 采用 Java 语言开发，采用MVC 架构。本文的区块链系统采用单机多节点部署模式。区 块链含有供应链中的农户部、原料厂商、生产厂商、零售和运输部门五家机构， 包含一 个排序节点，用于对数据进行排序和生成块。

5.5.2 系统功能展示

1）登录功能展示

提供用户的登录和注册功能，新用户可在注册页面填写相关信息，提交后在数据库 中添加新数据，注册成功后，在登录页面完成身份信息校验，校验成功后可登录溯源系

统，同时消费者用户无需登录，可直接根据溯源码查看溯源信息，如图 5-7 所示。

2）信息录入功能展示

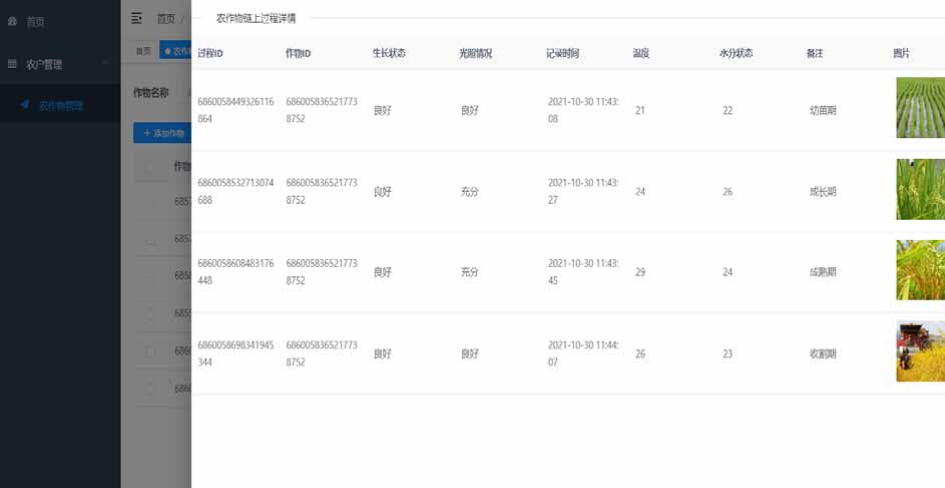
系统操作页面包括系统管理、系统监控、农户管理、物流管理、原料厂管理、生产 加工管理以及零售管理等 7 个模块。



图 5-7 系统登录页面

Figure 5-7 System login page

图 5-8 显示了有机大米溯源系统工作界面。图 5-8(a)为农户管理模块有机大米生长 信息的采集，图 5-8(b)为原料厂商存储有机大米的相关信息，图 5-8(c)为生产加工模块 的信息采集，图 5-8(d)为零售商上传的有机大米销售信息。



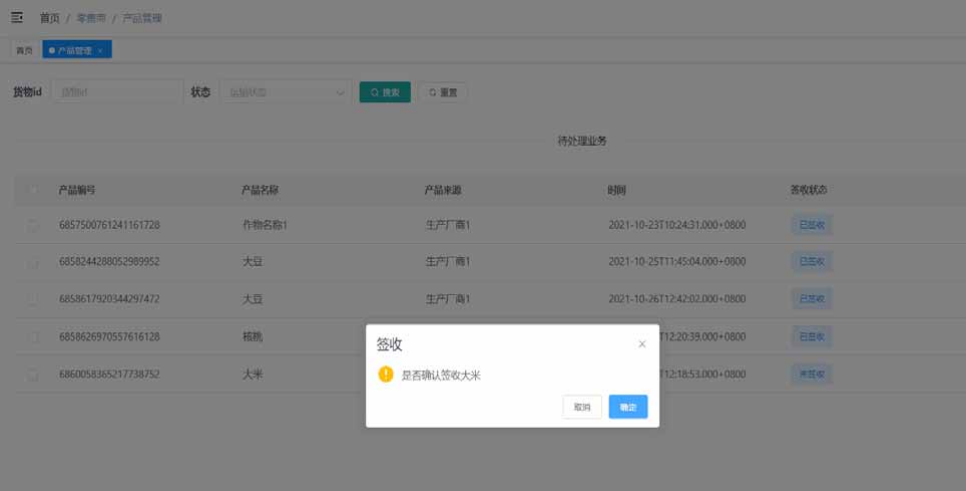
a.农户上传有机大米生长信息



b.原料厂商上传有机大米存储信息



c.生产商上传有机大米加工信息



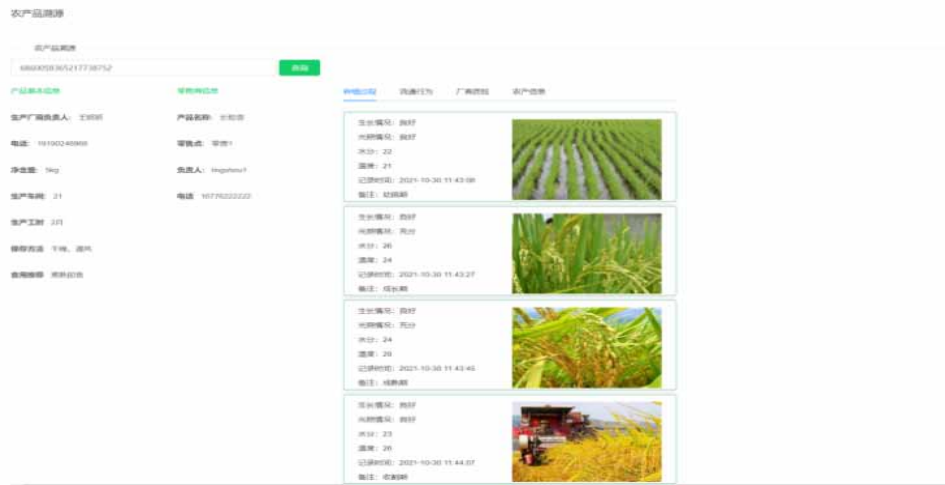
d.零售商上传有机大米出售信息

图 5-8 溯源系统工作界面

Figure 5-8 Working interface of traceability system

3）信息查询功能展示

图 5-9 展示了有机大米信息查询的方法。消费者以及相关监督部门通过输入包装上 的溯源码，向后台服务器发送查询请求，获取有机大米的相关追溯信息，包括种植信息、 有机大米流通信息、生产加工信息、厂商质检信息、零售信息等。该平台可以追溯大米 从种植到消费的整个生命周期，保障消费者掌握几乎所有信息的权利，透明化有机大米 的种植、生产和加工， 也能够增加消费者和企业之间的信任。此外， 区块链技术的应用 还可以有效地防止数据篡改。总而言之， 基于区块链技术搭建的平台实现了有机大米信 息的可追溯性，增加了商家、消费者之间的信任， 使双方利益最大化，同时也为科研人 员和企业提供了借鉴意义。



a.有机大米种植详情信息 b.有机大米生产厂商质检信息 图 5-9 有机大米溯源结果

Fig. 5-9 Traceability results of organic rice

4）系统监测功能展示

网络监控模块为用户提供区块链溯源系统的详情统计和数据分析功能。统计的信息 包括溯源链的区块信息、节点状态和交易记录。在网络监控模块， 后台提供的接口可以 返回不同时间段统计后的详情信息，统计数据将会用折线图、饼状图展示， 网络监控功 能模块界面如图 5-10 所示。

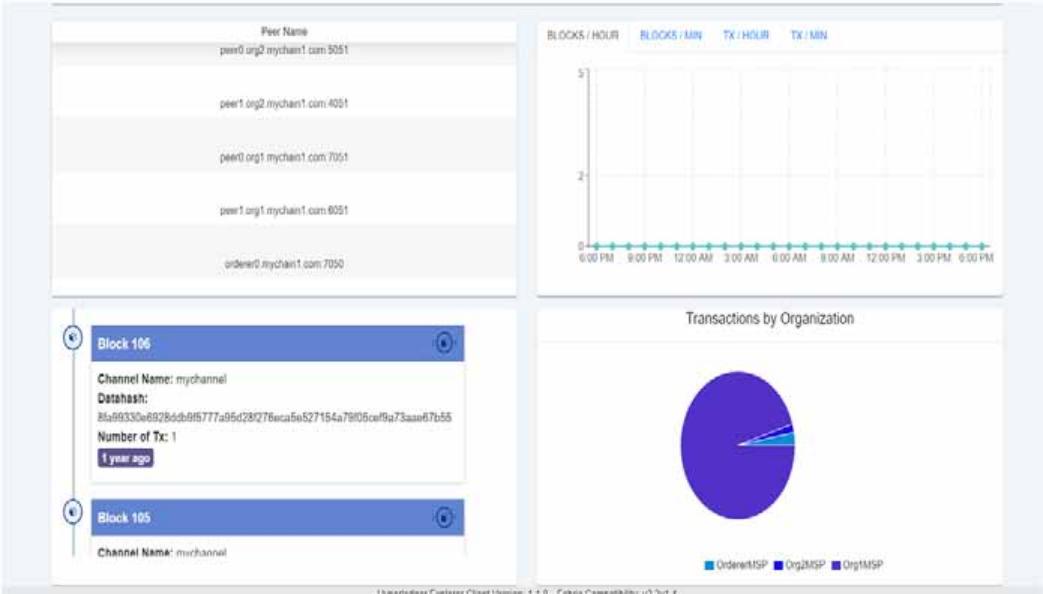
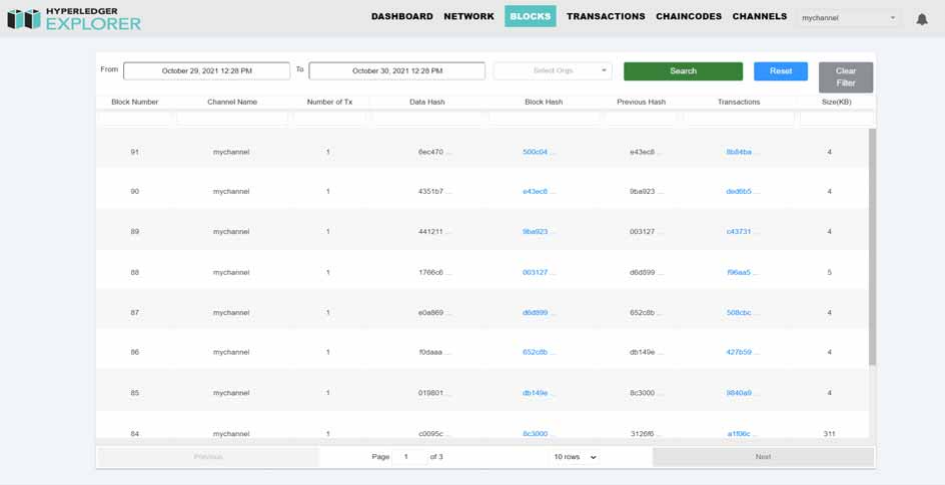
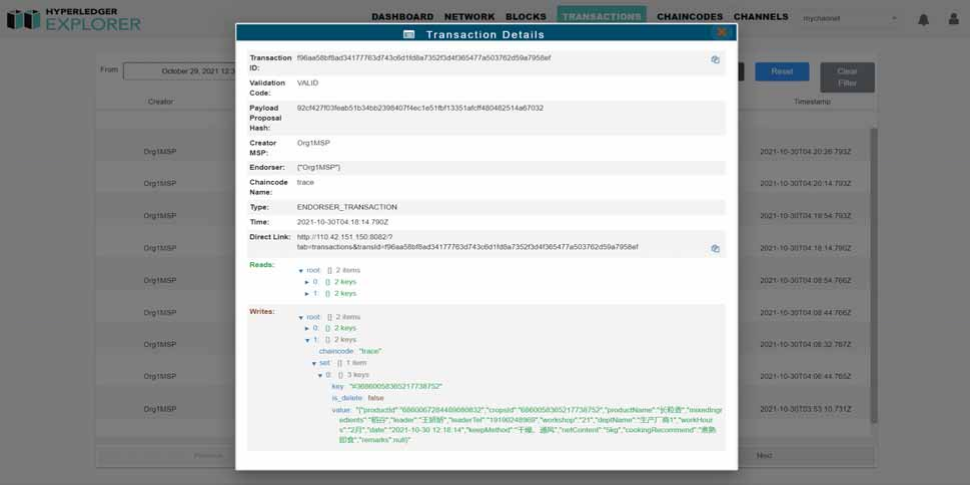


图 5-10 网络监控界面

Figure 5-10 Network monitoring interface

图 5-11 是区块链浏览器。系统管理员可以实时查看区块链的相关信息，如节点数、 合约数、区块数、交易数等。图 5-11(a)为区块列表界面，包含区块编号、通道名、交易 数量、数据哈希、区块哈希、前一区块哈希、交易哈希以及区块大小。图 5-11(b)为某一 交易详细信息界面，包含交易 ID、智能合约名、类型、创建时间、读写集等。



a. 区块列表界面 b.交易详情界面

图 5-11 区块链浏览器界面

Figure 5-11 Blockchain browser interface

5.6 本章小结

本章以第三章完成的溯源方案设计、模型构建和第四章完成的改进算法为指导， 成 功地以有机大米为例实现了农产品溯源系统的开发与测试工作。首先交代了系统的需求， 然后聚焦于溯源系统的具体模块，就功能、业务流程及系统架构进行了详细的分析、设 计，完成了基于区块链的农产品溯源系统，证明该农产品溯源系统基本能够达到既定目 标，基本能够实现关键功能，且无明显漏洞。

第 6 章 结论与展望

6.1 结论

本文的研究主要围绕传统农产品溯源领域存在的一些问题，包括数据集中存储、缺 乏监管、数据不公开透明、易于篡改等。这些问题导致农产品质量问题频发， 如以次充 好、假冒伪劣等现象， 进一步引发了消费者和商家之间的信任问题，结合当下较流行的 区块链技术，提出了基于区块链的农产品溯源方案。区块链为农产品溯源提供了可靠的 数据支持，但农产品溯源领域数据量大且供应链复杂，已有的共识算法不能很好地解决 系统吞吐量低、通信开销大、交易时延长等问题。针对这些问题， 本文设计了基于区块 链的农产品溯源方案、构建了模型和适用于农产品溯源的改进 PBFT 共识算法以及基于 区块链的农产品溯源平台。本文的主要研究结论包括以下几点：

1）通过分析大量文献，发现农产品溯源领域面临着数据存储不安全、不可信等问 题，提出了一种基于区块链的农产品溯源方案和模型，结合农产品供应链的全过程，定 制化设计了数据管理模式和智能合约。该方法框架为农产品的溯源和监管提供了理论基 础，并建立了消费者和商家之间的信任机制。

2）针对目前农产品溯源与区块链技术相结合的应用中存在的时延高、系统开销大、 支持的规模小等问题，提出了基于分组和信用投票的改进实用拜占庭容错算法 T-PBFT。 该算法结合农产品供应链的特点，优化了原算法中的一致性协议，提出了信用模型与投 票机制，为农产品溯源系统提供了更小的延迟、更高的吞吐量、更小的通信开销和更大 的拜占庭容忍度，可以支持更大规模的追溯，有效地改善网络节点间通信量急剧增加的 问题，减少恶意节点的影响。

3）在超级账本基础之上构建了有机大米溯源系统。该系统展示了有机大米追溯过 程中所涉及到的各个功能模块，并且验证了基于区块链技术的农产品溯源的可行性和有 效性。这种基于区块链技术的追溯系统为保障农产品安全提供了一种可靠的手段，并且 能够建立消费者与生产商之间的信任。

6.2 展望

目前，农产品溯源方面的区块链技术应用尚未成熟。因此， 本文基于区块链的农产 品溯源系统仍有优化空间，可以通过以下几个方面进行后续研究和改进：

1）针对农产品溯源领域的性能要求，本文改进了 PBFT 共识算法，并通过实验证明

改进的共识机制在数据确认和网络安全等方面有了一定程度的提高。但实验时间有限， 未来，需要探索更全面的算法比较方式，以进一步改进共识算法和提高系统的性能。

2）随着智能手机的更新换代和普及率的提高，下一步将进行区块链溯源 APP 和微 信小程序的研发。用户将能够随时随使用系统，提高系统的实用性。

参考文献

[1] 霍红, 钟海岩. 农产品供应链质量安全中区块链技术投入的演化分析[J]. 运筹与管 理, 2023, 32(01):15-21.

[2] 任文, 郭玉鹏. 基于电商的食品溯源及推荐平台的设计与实现[J]. 电脑与信息技术, 2020, 28(05):27-29.

[3] 陆秋俊. 物联网技术在食品溯源中的应用研究[J]. 物联网技术, 2019,9(11):83-85.

[4] 陆秋俊. 基于物联网技术构建现代农业种植及食品溯源系统[J]. 现代农业科技, 2019(22):252-253.

[5] Liu S, Zhang R, Liu C, et al. Improvement of the PBFT Algorithm Based on Grouping and Reputation Value Voting[J]. International Journal of Digital Crime and Forensics (IJDCF), 2022, 14(3):1-15.

[6] 张亮, 刘百祥, 张如意, 等. 区块链技术综述[J]. 计算机工程, 2019,45(05):1-12.

[7] 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(04):1-7.

[8] Liu S, Zhang R, Liu C, et al. P-PBFT: An improved blockchain algorithm to support large- scale pharmaceutical traceability[J]. Computers in Biology and Medicine, 2023, 154:106590.

[9] 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.

[10]古银花. 手机二维码在农产品溯源中的应用研究[J]. 市场研究, 2013(04):20-21.

[11] Gandino F, Montrucchio B, Rebaudengo M, et al. On improving automation by integrating RFID in the traceability management of the agri-food sector[J]. IEEE Transactions on Industrial Electronics, 2009, 56(7):2357-2365.

[12]Cheng C, Jiang P, Liu J. A common traceability method for agricultural products based on data center[J]. Sensor Letters, 2013, 11(6-7):1269-1273.

[13]Costa C, Antonucci F, Pallottino F, et al. A review on agri-food supply chain traceability by means of RFID technology[J]. Food and bioprocess technology, 2013, 6:353-366.

[14]Fu H, Zhao C, Cheng C, et al. Blockchain-based agri-food supply chain management: case study in China[J]. International Food and Agribusiness Management Review, 2020, 23(5):667-679.

[15]Shi X, Zhuge H. Cyber physical socio ecology[J]. Concurrency and computation: Practice and Experience, 2011, 23(9):972-984.

[16]Ying F, Fengquan L. Application of internet of things to the monitoring system for food

quality safety[C]. //Proceedings of the 4th International Conference on Digital Manufacturing & Automation. Shinan, China: IEEE, 2013: 296-298.

[17]Radogna A V, Latino M E, Menegoli M, et al. A Monitoring Framework with Integrated Sensing Technologies for Enhanced Food Safety and Traceability[J]. Sensors, 2022, 22(17):6509.

[18]黄友文 . 基于 RFID 及物联网技术的茶叶溯源系统研究 [J]. 保鲜与加工 , 2016,16(04):112-117.

[19]陶佰睿, 赵金利, 李雪, 等. 基于 Kmeans 改进 FP 算法稻米溯源体系优化设计[J]. 安 徽农业大学学报, 2019, 46(01):198-202.

[20]Salah K, Nizamuddin N, Jayaraman R, et al. Blockchain-based soybean traceability in agricultural supply chain[J]. Ieee Access, 2019, 7:73295-73305.

[21]Hu S, Huang S, Huang J, et al. Blockchain and edge computing technology enabling organic agricultural supply chain: A framework solution to trust crisis[J]. Computers & Industrial Engineering, 2021, 153:107079.

[22]Monteiro E S, Da Rosa Righi R, Barbosa J L V, et al. APTM: A model for pervasive traceability of agrochemicals[J]. Applied Sciences, 2021, 11(17):8149.

[23]HaleemA, Khan S, Khan M I. Traceability implementation in food supply chain: A grey- DEMATEL approach[J]. Information Processing in Agriculture, 2019, 6(3):335-348.

[24]Shurman M, Obeidat A A, Al-Shurman S A. Blockchain and smart contract for IoT[C]. //2020 11th International Conference on Information and Communication Systems (ICICS). Irbid, Jordan: IEEE, 2020: 361-366..

[25]Surasak T, Wattanavichean N, Preuksakarn C, et al. Thai agriculture products traceability system using blockchain and internet of things[J]. International Journal of Advanced Computer Science and Applications, 2019, 10(9): 268-272.

[26]Wang L, Xu L, Zheng Z, et al. Smart contract-based agricultural food supply chain traceability[J]. IEEE Access, 2021, 9:9296-9307.

[27]Yang X, Li M, Yu H, et al. A trusted blockchain-based traceability system for fruit and vegetable agricultural products[J]. IEEE Access, 2021, 9:36282-36293.

[28]Yiu N C. Decentralizing supply chain anti-counterfeiting and traceability systems using blockchain technology[J]. Future Internet, 2021, 13(4):1-33.

[29]Tian F. 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). IEEE, 2016:1-6.

[30]Lin Q, Wang H, Pei X, et al. Food safety traceability system based on blockchain and EPCIS[J]. IEEE Access, 2019, 7:20698-20707.

[31]Baralla G, Pinna A, Corrias G. Ensure traceability in European food supply chain by using a blockchain system[C]. //2019 IEEE/ACM 2nd International Workshop on Emerging

Trends in Software Engineering for Blockchain (WETSEB). IEEE, 2019:40-47.

[32]Fei C, Chunming Y, Tao C. Design of food traceability system based on blockchain[J]. Computer Engineering and Applications, 2021, 57(02):60-69.

[33]Dey S, Saha S, SinghAK, et al. FoodSQRBlock: Digitizing food production and the supply chain with blockchain and QR code in the cloud[J]. Sustainability, 2021, 13(6):3486.

[34]Dey S, Saha S, Singh A K, et al. SmartNoshWaste: Using blockchain, machine learning, cloud computing and QR code to reduce food waste in decentralized web 3.0 enabled smart cities[J]. Smart Cities, 2022, 5(1):162-176.

[35]WANG K, CHEN Z, XU J. Efficient traceability system for quality and safety of agricultural products based on consortium blockchain[J]. Journal of Computer Applications, 2019, 39(8):2438.

[36]Gao Q, Yang C, Wu X, et al. Research on the traceability system of tea quality and safety based on blockchain[J]. Journal of Anhui Agricultural University, 2021, 48:299-303.

[37]You Y, Kong L, Xiao Z, et al. Hybrid indexing scheme supporting blockchain transaction tracing[J]. Computer Integrated Manufacturing Systems, 2019, 25(04):978-984.

[38]Yao Q, Zhang H. Improving Agricultural Product Traceability Using Blockchain[J]. Sensors, 2022, 22(9):3388.

[39]Kuo T, Kim H, Ohno-Machado L. Blockchain distributed ledger technologies for biomedical and health care applications[J]. Journal of the American Medical Informatics Association, 2017, 24(6):1211-1220.

[40]Hu T, Liu X, Chen T, et al. Transaction-based classification and detection approach for Ethereum smart contract[J]. Information Processing & Management, 2021, 58(2):102462.

[41]Di J, Zang Q. Research on Drug Supervision System Based on Fisco Bcos Blockchain[J]. Frontiers in Business, Economics and Management, 2021, 2(3):109-111.

[42]姚影, 颜拥, 郭少勇, 等. 基于联盟链的分布式高效身份认证[J]. 电子技术应用, 2022, 48(03):104-108.

[43]Aung M M, Chang Y S. Traceability in a food supply chain: Safety and quality perspectives[J]. Food Control, 2014, 39:172-184.

[44]马春光, 安婧, 毕伟, 等. 区块链中的智能合约[J]. 信息网络安全, 2018(11):8-17.

[45]贺海武, 延安, 陈泽华. 基于区块链的智能合约技术与应用综述[J]. 计算机研究与 发展, 2018, 55(11):2452-2466.

[46]季超越, 郭仲勇, 岳勇. 超级账本智能合约的应用研究[J]. 现代信息科技, 2020, 4(04):176-179.

[47]Wang Y, Singgih M, Wang J, et al. Making sense of blockchain technology: How will it transform supply chains?[J]. International Journal of Production Economics, 2019, 211:221-236.

[48]韩璇, 刘亚敏. 区块链技术中的共识机制研究[J]. 信息网络安全, 2017(09):147-152.

[49]Jiang Y, LianZ. High performance and scalable byzantine fault tolerance[C]. //Proceedings of 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC). IEEE, 2019:1195-1202..

[50]郑敏, 王虹, 刘洪, 等. 区块链共识算法研究综述[J]. 信息网络安全, 2019(07):8-24.

[51]戴安博, 陈恭亮. POW 区块链共识算法分析与展望[J]. 通信技术, 2019, 52(12):2839- 2845.

[52]谭敏生, 杨杰, 丁琳, 等. 区块链共识机制综述[J]. 计算机工程, 2020, 46(12):1-11.

[53]Li Y, Qiao L, Lv Z. An optimized byzantine fault tolerance algorithm for consortium blockchain[J]. Peer-to-Peer Networking and Applications, 2021, 14(5):2826-2839.

[54]Wang Y, Cai S,LinC, et al. Study of blockchains’s consensus mechanism based on credit[J]. IEEE Access, 2019, 7:10224-10231.

[55]Gao Z, Yang L. Optimization Scheme of Consensus Mechanism Based on Practical Byzantine Fault Tolerance Algorithm[J]. Blockchain Technology and Application: Second CCF China Blockchain Conference (CBCC 2019), 2020, 1176:187-195.

[56]谢卓, 张志鸿, 李磊, 等. 基于联盟链的实用拜占庭容错算法的改进[J]. 计算机科学, 2022, 49(11):360-367.

[57]Behnke K, Janssen M F W H. Boundary conditions for traceability in food supply chains using blockchain technology[J]. International Journal of Information Management, 2020, 52:101969.

[58]Feng L, Zhang H, Chen Y, et al. Scalable Dynamic Multi-Agent Practical Byzantine Fault- Tolerant Consensus in Permissioned Blockchain[J]. Applied Sciences-Basel, 2018, 8(10):1919.

[59]Li W, Feng C, Zhang L, et al. A Scalable Multi-Layer PBFT Consensus for Blockchain[J]. IEEE Transactions on Parallel and Distributed Systems, 2021, 32(5):1146-1160.

[60]SankaAI, Cheung R C C. A systematic review of blockchain scalability: Issues, solutions, analysis and future research[J]. Journal of Network and Computer Applications, 2021, 195:103232.

[61]卢丽, 孙林夫, 邹益胜. 基于一致性哈希环多主节点的改进实用拜占庭容错算法[J]. 计算机集成制造系统, 2023, 29(01):25-35.

[62]王弘洁. 智慧医疗场景下基于联盟区块链的跨域身份认证[D]. 南京邮电大学, 2021.

[63]方燚飚, 周创明, 李松, 等. 联盟链中实用拜占庭容错算法的改进[J]. 计算机工程与 应用, 2022, 58(03):135-142.

[64]高灿. 基于区块链的农产品溯源应用研究[D]. 河北科技师范学院, 2022.

[65]Zheng Z, Xie S, Dai H, et al. Blockchain challenges and opportunities: a survey[J]. International Journal of Web and Grid Services, 2018, 14(4):352-375.

[66]蒲松涛, 刘倩. 全球公有链技术评估及指数编制[J]. 网络空间安全, 2018, 9(10):1-6.

[67]Morkunas V J, Paschen J, Boon E. How blockchain technologies impact your business

model[J]. Business Horizons, 2019, 62(3):295-306.

[68]Yang L. The blockchain: State-of-the-art and research challenges[J]. Journal of Industrial Information Integration, 2019, 15:80-90.

[69]Galvez J F, Mejuto J C, Simal-Gandara J. Future challenges on the use of blockchain for food traceability analysis[J]. TrAC Trends in Analytical Chemistry, 2018, 107:222-232.

[70]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.

[71]Kamble S S, Gunasekaran A, Gawankar S A. Achieving sustainable performance in a data- driven agriculture supply chain: A review for research and applications[J]. International Journal of Production Economics, 2020, 219:179-194.

[72]Xiong W, Xiong L. Smart Contract Based Data Trading Mode Using Blockchain and Machine Learning[J]. IEEE Access, 2019, 7:102331-102344.

[73]Castro M, Liskov B. Practical byzantine fault tolerance[C]. //Proceedings of the 3rd Symposium on Operating Systems Design and Implementation. 1999, 99:173-186.

[74]Bocek T, Rodrigues B B, Strasser T, et al. Blockchains everywhere-a use-case of blockchains in the pharma supply-chain[C]. //Proceedings of the 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM). IEEE, 2017:772-777.

[75]Jamil F, Hang L, Kim K, et al. A Novel Medical Blockchain Model for Drug Supply Chain Integrity Management in a Smart Hospital[J]. Electronics, 2019, 8(5):505.

[76]Alangot B, Achuthan K. Trace and track: Enhanced pharma supply chain infrastructure to prevent fraud[C]. //Proceedings of the First International Conference on Ubiquitous Communications and Network Computing (UBICNET 2017). Springer International Publishing, 2018:189-195.

[77]Jun G, Li Q, Zihao C. Improvement of Byzantine fault tolerant consensus algorithm for blockchain[J]. Computer Applications, 2019, 39(07):2148-2155.

[78]Zhang Z, Zhu D, Fan W. Qpbft: practical byzantine fault tolerance consensus algorithm based on quantified-role[C]. //Proceedings of the 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). IEEE, 2020:991-997.

[79]Mirabelli G, Solina V. Blockchain and agricultural supply chains traceability: research trends and future challenges[J]. Procedia Manufacturing, 2020, 42:414-421.

[80]Li Y, Qiao L, Lv Z. An Optimized Byzantine Fault Tolerance Algorithm for Consortium Blockchain[J]. Peer-to-Peer Networking and Applications, 2021, 14:2826-2839.