塔里木大学
TARIM UNIVERSITY

# 基于区块链技术的农产品溯源关键技术研究

## 开题报告

汇报人：柏小康

时　间：2024.11.10

# \目 录
CONTENT

# 一、选题背景及意义

## 1.1 研究背景

01

### 农产品溯源难

随着社会经济发展和生活水平提升，食品安全备受瞩目，食用农产品质量直接影响消费者健康。但频发的安全问题损害市场信任。传统农产品溯源系统存弊端，难以以满足需求。农产品供应链复杂，包含多参与者和数据，安全监督和可追溯性挑战大。

02

### 区块链助溯源

区块链技术凭其去中心化、不可篡改和透明性，为农产品溯源提供新解。自比特币问世，区块链在多个领域获广泛应用。结合农产品溯源，可确保数据真实、提高消费者信任。习总书记亦强调区块链与传统行业结合，推动“区块链+”建设。

03

### 联盟链溯源

区块链分三类，联盟链适合农产品追溯，因其成员间有限访问和高效交易。国家加密算法各异，Hyperledger Fabric虽有影响，但缺国密支持且算法扩展受限，需依行业规范和法律调整加密算法。

# 一、选题背景及意义

## 1.1 研究背景


01

**数据存储和管理：**传统的中心化数据库存在单点故障和数据篡改的风险，而区块链技术可以实现数据的去中心化存储和管理。

02

**数据隐私和安全：**农产品溯源数据涉及到生产者、供应商和消费者的隐私信息，需要采用加密算法确保数据的安全性和隐私保护。

03

**系统性能和扩展性：**区块链技术在实际应用中面临性能和扩展性的挑战，需要通过优化算法和架构设计来提高系统性能和扩展性。

# 一、选题背景及意义

## 1.2 研究意义

### 研究意义一

农产品追溯机制的实施显著提高了追踪效率，确保了食品安全与品质，同时通过验证产品真伪支撑了价格合理性，降低了欺诈。然而，线上交易平台众多且管理模式单一，质量检测难以全面覆盖。我国农业部门正构建追溯系统以解决此问题。传统溯源系统多为中心化平台，虽操作简便，但数据安全和监管手段不足，存在篡改和数据安全风险。

### 研究意义二

本文通过对溯源方案进行区块链技术设计，并开发Web应用程序，构建了一个农产品溯源信息系统，旨在加强农产品全过程管理，保障食品安全。该研究提升了溯源系统的可信度和效率，增强了消费者信任，促进了农业生产的数字化转型，提升了生产效率和管理水平，为其他领域的应用提供了有益参考。

# 一、选题背景及意义

## 1.3 国内外发展现状

**国内外发展现状**

### 传统农产品溯源研究现状

农产品溯源技术利用现代信息技术，全程记录农产品从种植到餐桌的各环节，对保障食品安全、提升消费者信任至关重要。国家政策方面，我国自1995年起实施相关法规，不断完善食品追溯体系。然而，传统溯源系统中心化程度高，存在数据安全问题，需进一步探索新技术解决。

### 基于区块链的农产品溯源研究现状

近年来，区块链技术在农产品溯源中备受关注，众多文献探讨了其在供应链可追溯性中的应用。尽管已有多种基于区块链的溯源系统被提出，但在存储容量、可伸缩性及数据保护上仍存局限。文献提出了优化方案，旨在提高系统效率、灵活性和数据隐私保护。

### 国内外研究现状总结

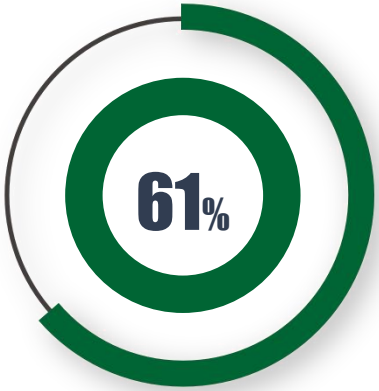
本文通过文献综述发现，区块链在农产品溯源中虽有进展但仍存性能、扩展性及数据隐私等问题。农产品追溯复杂且现有系统多为中心化，存在安全、可追溯性及可靠性问题。区块链虽提供安全访问环境，但面临交易处理、安全性及隐私泄露挑战，需结合应用以确保安全性、可追溯性及不变性。

# 二、研究方案

## 2.1 研究目标


构建一个基于区块链技术的农产品溯源平台，通过区块链技术确保农产品数据的安全性、可追溯性、不变性和可达性。解决现有区块链溯源系统中存在的性能和扩展性、数据隐私保护等问题。


保障食品安全，通过农产品追溯，迅速确定农产品的生产来源和分销渠道，帮助识别和解决食品安全问题。




实现农产品从生产到消费全过程的信息可追溯和可共享，保障食品安全，增强消费者信任。

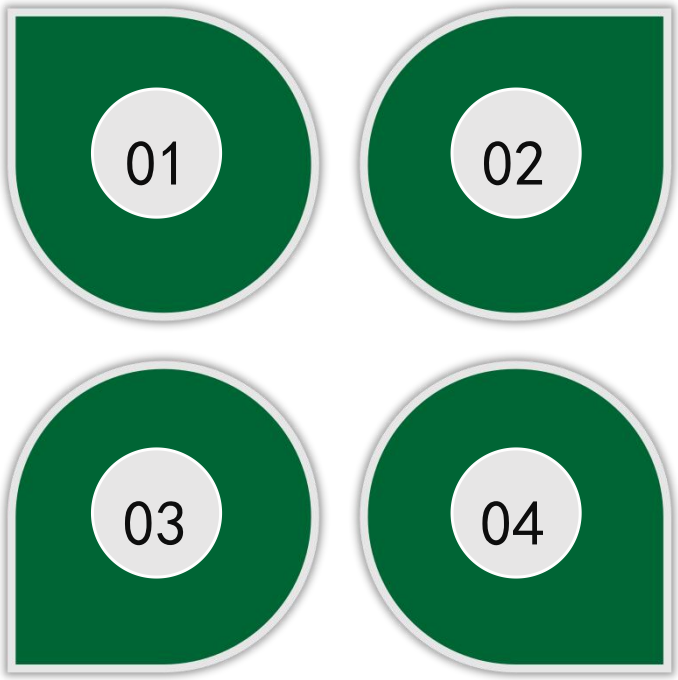

促进农业现代化，通过数字化转型，提升农业生产效率和管理水平。

# 二、研究方案

## 2.2.1 研究内容

### 设计基于区块链的农产品溯源方案

研究区块链在农产品溯源中的应用，设计基于区块链的溯源方案，结合传统体系，解决信息不透明、数据易篡改问题。




### 构建区块链+IPFS农产品溯源信息模型

研究IPFS分布式存储，结合区块链构建农产品溯源模型，IPFS存大文件，区块链存摘要，实现去中心化存储管理。

### Fabric平台国密算法嵌入设计思路

基于同济开源国密，为Fabric平台添加SM2/SM3/SM4算法，提出数据记录存储方案，提高数据安全性、隐私保护及完整性。

### 设计基于区块链的农产品信息溯源系统

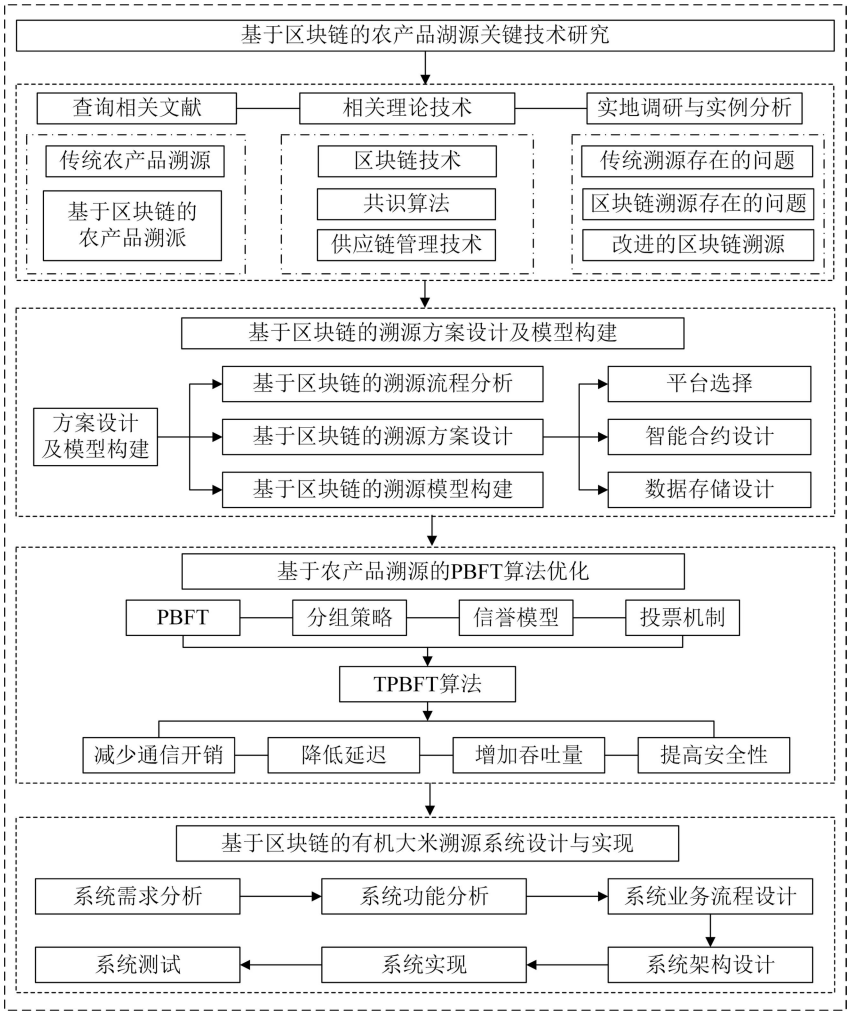
搭建区块链环境，开发Web应用，实现农产品溯源系统，测试性能，确保从农场到餐桌的信息可追溯共享，验证方案可行。

# 二、研究方案

## 2.2.2 技术路线

首先深入探讨了传统与区块链农产品溯源技术，研究了区块链技术、共识算法及供应链管理等相关理论。通过实地调研与实例分析，我们识别了两种溯源方式存在的问题，并提出了改进的区块链溯源方案。随后，我们设计了基于区块链的溯源方案及模型，并嵌入了国密算法以提高系统安全性。最终，采用Hyperledger Fabric和IPFS技术，我们开发了Web应用程序，实现了基于区块链的农产品溯源系统，并进行了系统需求分析、测试和功能实现。

### 技术路线图



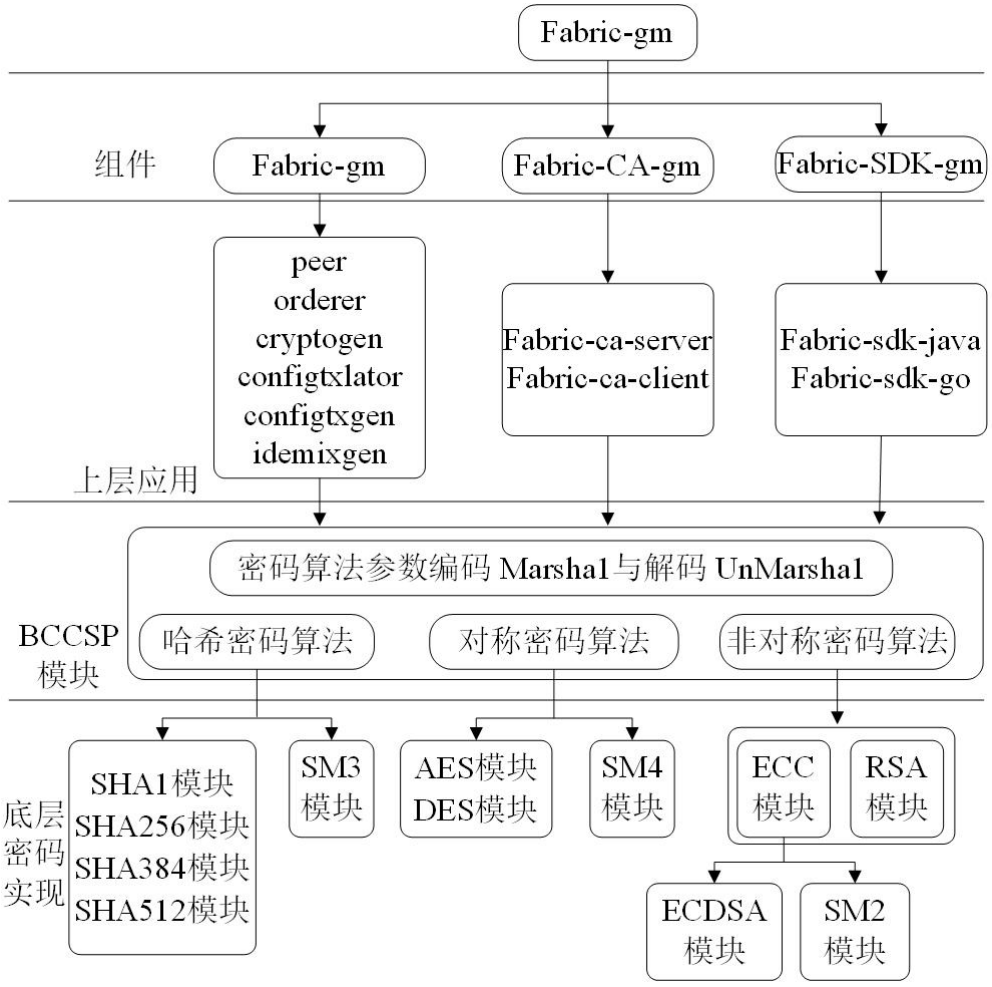
# 二、研究方案

## 2.3.1 实验方案

本研究设计基于区块链的农产品溯源方案，构建区块链+IPFS溯源信息模型，利用IPFS分布式存储，并在Fabric平台嵌入国密算法，提出数据记录存储方案，提升系统安全性。

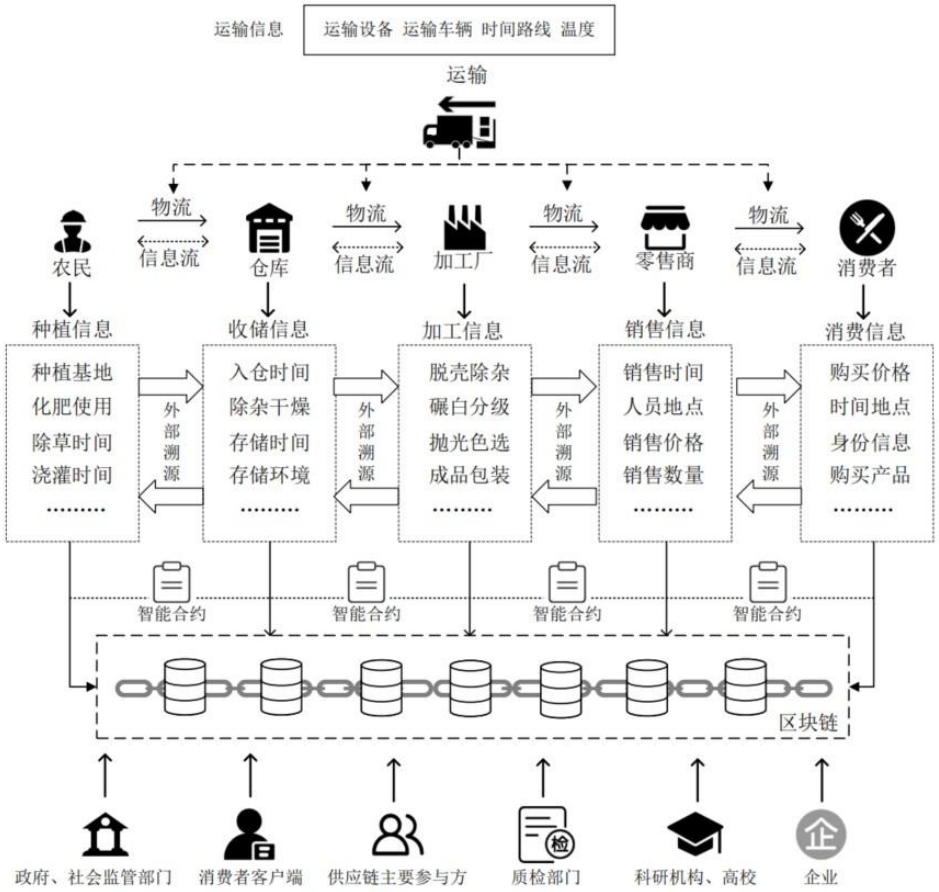
实验方案考虑农产品供应链溯源流程，涵盖种植到消费各环节，通过智能合约和物流信息流记录传递各环节信息，确保数据透明不可篡改。

### 国密算法嵌入设计思路图

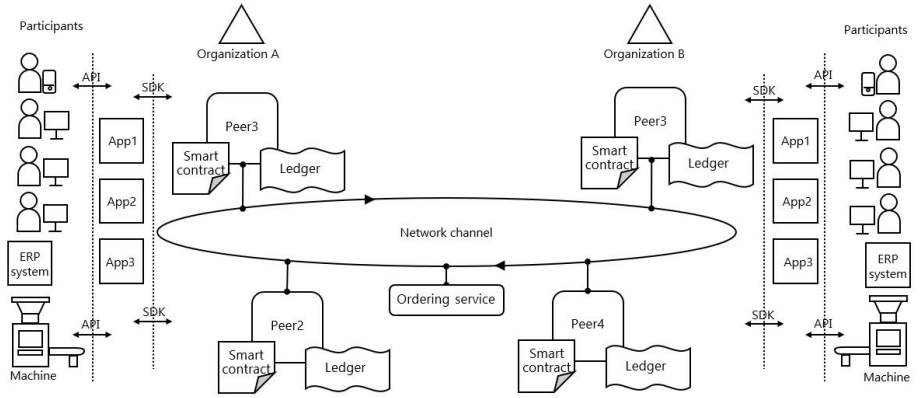


# 二、研究方案

## 2.3.1 实验方案




农产品供应链溯源流程图




使用hyperleger 实现的业务网络

最终，我们基于Hyperledger Fabric搭建区块链环境，设计并实现农产品溯源信息模型，开发Web应用，进行系统功能及性能测试，确保其安全性、可靠性和高效性

# 二、研究方案

## 2.3.2 可行性分析

### 确定可行性

分析区块链技术和农产品溯源需求，确认研究方案可行。区块链在溯源领域有成功案例，Hyperledger Fabric框架成熟适用企业级应用，IPFS解决存储瓶颈，国密算法提升数据安全，符合国家政策，整体方案具备高度可行性。

### 技术、经济和社会可行性

技术可行性上，区块链与IPFS技术成熟度高；经济可行性上，数字化转型提升农业效率，降低成本；社会可行性上，增强农产品溯源可信度，保障食品安全。综上，本研究方案在技术、经济和社会三方面均可行，确保目标实现。

# 二、研究方案

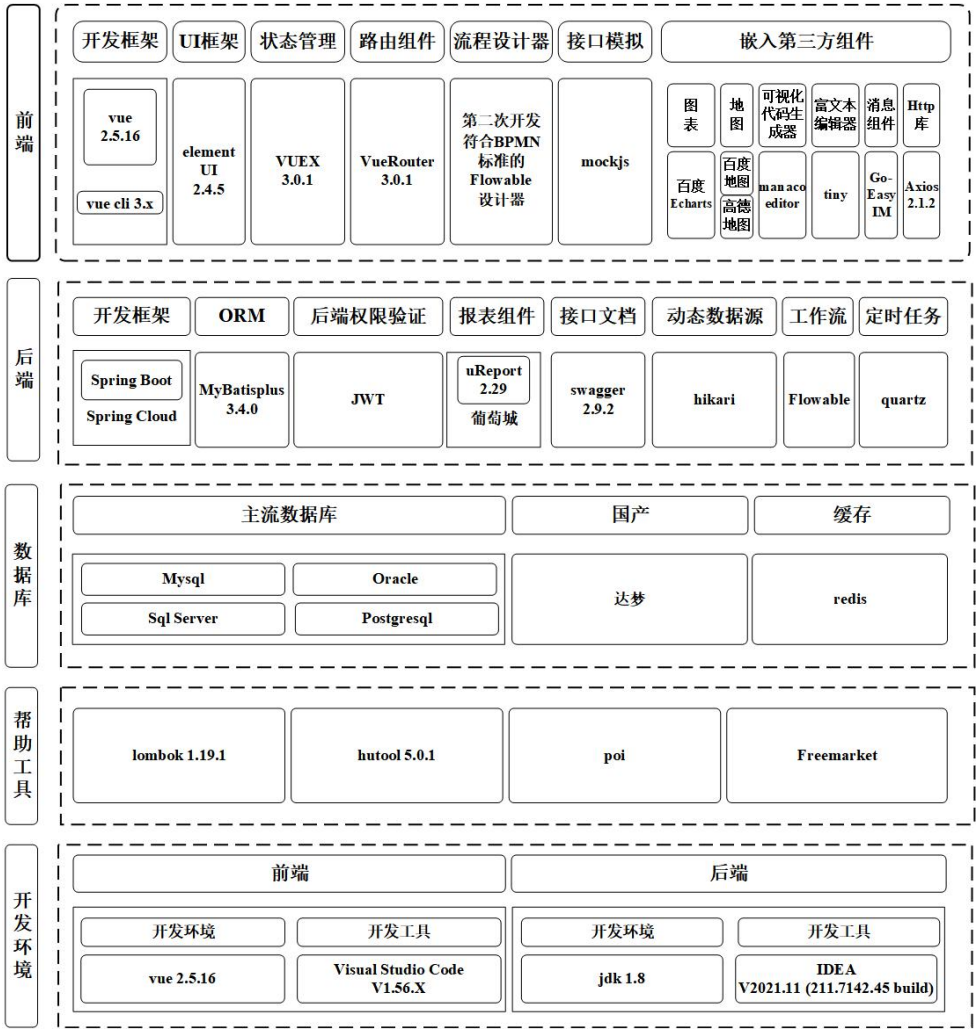
## 2.3.3 准备工作及现有条件

农产品溯源系统研究前，需充分准备。技术层面，需精通区块链、IPFS及国密算法，保障数据安全；资源层面，需配备服务器、网络环境等硬件，以及区块链开发平台、IPFS节点等软件工具，确保研究目标顺利实现。

| 模块 | 工具 |
| --- | --- |
| 操作系统 | Ubuntu 20.04 LTS |
| 区块链平台 | Hyperledger Fabric V2.2.15 |
| 智能合约语言 | Go 1.23.1 |
| 其他工具 | Docker、Caliper等 |

开发工具表

技术架构采用Hyperledger Fabric V2.2与IPFS，结合力软JAVA快速开发平台和运维开发一体化平台。依托现有区块链成果、开源项目及农产品溯源经验，确保研究方案可行实用。




力软JAVA快速开发平台技术栈

# 二、研究方案

## 2.3.4 可能遇到的困难和问题与解决途径

### 区块链技术的性能和扩展性问题

区块链技术在实际应用中面临性能和扩展性的挑战，过优化区块链网络结构和算法，提高系统性能和扩展性。

### 数据隐私保护问题

农产品溯源数据涉及到生产者、供应商和消费者的隐私信息，通过嵌入国密算法，确保数据的安全性和隐私保护。

### 系统集成和测试问题

通过详细的系统设计和测试计划，确保系统的稳定性和可靠性。

# 三、预期达到的目标和主要创新点

## 3.1本研究的预期目标

### 提升系统效率与可信度

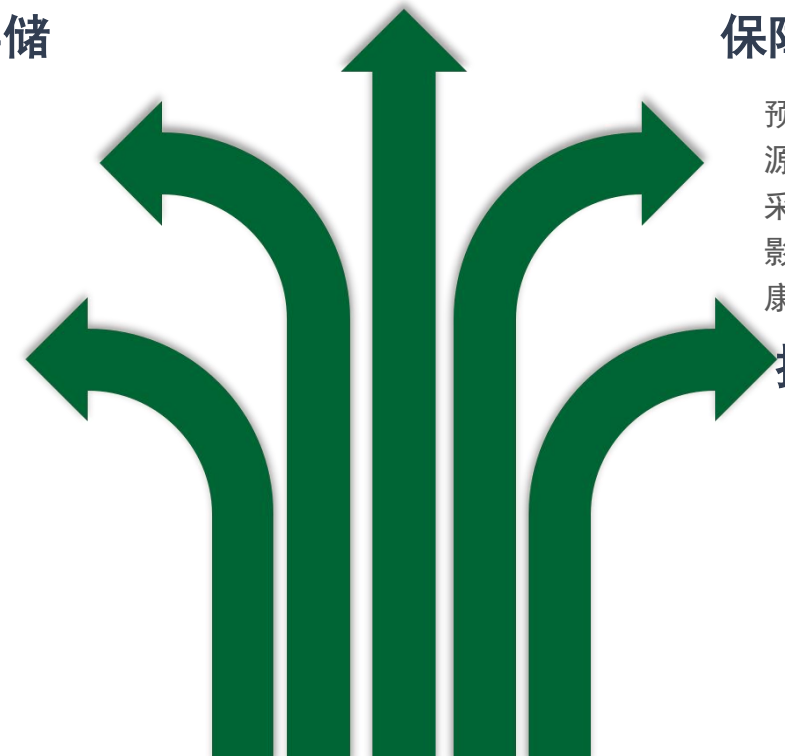
系统设计旨在优化区块链网络及数据处理流程，提升溯源系统运行效率，并确保数据不可篡改，增强系统可信度，使消费者和供应链参与者更信赖溯源信息。

### 确保数据安全与去中心化存储

在Fabric上集成国密算法，提升数据安全至最高标准，用IPFS去中心化存储数据，增强抗篡改能力，提高农产品溯源系统的可信度。

### 保障食品安全与响应速度

预期的效果包括能够迅速通过溯源系统定位食品安全问题，及时采取措施，减少食品安全事件的影响。这将有助于保护消费者健康，同时提升农产品品牌形象。



### 建立全面的溯源信息模型

目标之一是构建区块链+IPFS的农产品溯源模型，记录共享从农田到餐桌的每一步信息，实现全生命周期透明化，为消费者和监管机构提供可追溯信息。

### 推动农业现代化与消费者信任

最终目标是应用区块链技术推动农业数字化转型，提高生产效率和管理水平，提供透明可靠农产品信息，增强消费者信任，促进农业市场健康发展。

# 三、预期达到的目标和主要创新点

## 3.2主要创新点

1

### 区块链与农产品溯源的结合

区块链技术的去中心化、不可篡改和透明性使其成为农产品溯源系统的理想选择，它能记录农产品从生产到销售的全过程数据，确保真实性和可追溯性，提高消费者信任度，助力企业快速定位和解决问题。

2

### 引入星际文件系统（IPFS）

为解决区块链系统存储资源浪费问题，本文提出“链上索引，链下存储”方案，将区块链数据索引存于Hyperledger Fabric，数据主体存于IPFS。此方案减轻存储压力，确保数据安全与可访问性。

3

### 在Fabric平台上嵌入国密算法

为增强数据安全与隐私保护，本文在Hyperledger Fabric平台嵌入SM2、SM3和SM4国密算法，它们在加密、签名和哈希函数上具有高安全性，有效防止数据篡改和泄露，提升整体安全性。

# 四、研究进度及时间安排

| 序号 | 开始日期 | 结束日期 | 主要工作内容（研究开发进度） |
|---|---|---|---|
| 1 | 2024年11月 | 2024年2月 | 研究背景调查和文献综述 |
| 2 | 2025年3月 | 2025年4月 | 设计基于区块链的农产品溯源方案 |
| 3 | 2025年5月 | 2025年6月 | 构建区块链+IPFS农产品溯源信息模型 |
| 4 | 2025年7月 | 2025年8月 | Fabric平台国密算法嵌入设计 |
| 5 | 2025年9月 | 2025年10月 | 设计基于区块链的农产品信息溯源系统 |
| 6 | 2025年11月 | 2026年3月 | 整理研究数据，撰写、修改论文 |
| 7 | 2026年4月 | 2026年6月 | 参加论文答辩 |

# 五、经费预算

| 支出科目 | 金额（万元） | 计算根据及理由 |
| --- | --- | --- |
| 出版/文献/信息传播/知识产权事务费 | 0.3 | 发表论文、申请软著；文献、检索、期刊订购等 |
| 实验材料费 | 0.2 | 自封袋、牛皮信封等实验耗材 |
| 差旅费 | 0.3 | 赴各实验基地采集数据 |
| 仪器设备费 | 0.2 | 服务器租赁、软件购买等费用 |

Thanks