



**毕业论文(设计)**

|  |  |
| --- | --- |
| **论文题目：** | **基于区块链的甘肃省中医药材管理系统** |
| **学 院：** | **数学与信息工程学院** |
| **年 级：** | **2019级** |
| **专 业：** | **计算机科学与技术** |
| **学 号：** | **2019051101** |
| **姓 名：** | **曹喜龙** |
| **指导教师：** | **姚云霞** |
| **完成时间：** |  |

**作者声明**

本毕业论文（设计）在姚云霞老师指导下由本人独立完成，没有剽窃、抄袭、造假等违反道德、学术规范和其他侵权行为。对本论文（设计）的研究做出重要贡献的个人和集体，均以在文中以明确方式标明。本毕业论文设计引起的法律结果完全由本人承担。

毕业论文（设计）成果归陇东学院所有。

特此声明。

作者专业：计算机技术与科学

作者学号：2019051101

作者签名：

年 月 日

基于区块链中医药材管理系统的设计与实现

**曹喜龙**

**（陇东学院数学与信息工程学院）**

Design and implementation of traditional Chinese medicine management system based on block chain

**Cao Xilong**

**(School of Mathematics and Information Engineering, Longdong University)**

**摘 要**

甘肃是全国中药材生产大省，也是全国中药材贸易大省。在生产和流通过程中，中药材的质量控制显得尤为重要。对此，省商务厅高度重视中药材流通追溯体系建设，努力从源头上把控好中药材的质量。同时，将中药材、蔬菜等追溯体系建设作为精准扶贫的重要举措来抓，畅通消费渠道，促进农民增产增收和脱贫致富。“甘肃的中药材品质优良，特别是当归、党参，被誉为药材之王，在马来西亚享有盛誉。”前不久在117届广交会上，马来西亚海鸥集团董事陈先生对甘肃的中药材赞不绝口。他说，公司从上世纪70年代开始就与甘肃开展中药材合作，药材品种涵盖当归、党参、大黄、黄芪、半夏、枸杞、甘草、锁阳等50多个品种。中成药从兰州佛慈制药、甘肃美迩康制药进口达到200多个品种，常规品种保持50多个。

但是随着甘肃省中药材的发展，中药材的质量把关也显得尤为重要。与食品安全问题一样，中药材安全在人们心中也显得尤为重要。在中药材采集加工的过程中，产生了诸如假冒伪劣产品，过期产品等问题。本系统利用区块链中不可篡改和重加密的特性，设计出一个比较完善的中药材管理系统。

**关键词：**区块链；加密算法；溯源系统；

**Abstract**

**Gansu is a major province in the production of Chinese herbal medicines and a major trader of Chinese herbal medicines in the country. In the process of production and circulation, the quality control of Chinese herbal medicines is particularly important. In this regard, the Provincial Department of Commerce attaches great importance to the construction of a traceability system for the circulation of Chinese herbal medicines, and strives to control the quality of Chinese herbal medicines from the source. At the same time, the construction of a traceability system for traditional Chinese medicinal materials and vegetables is taken as an important measure for targeted poverty alleviation, unblocking consumption channels, and promoting farmers to increase production and income and get rid of poverty and become rich. "Gansu's Chinese medicinal materials are of high quality, especially angelica and Codonopsis pilosula, known as the king of medicinal materials and enjoying a high reputation in Malaysia." Not long ago, at the 117th Canton Fair, Mr. Chen, director of Malaysia Seagull Group, was full of praise for Gansu's Chinese medicinal materials. He said that the company has cooperated with Gansu on Chinese medicinal materials since the 1970s, covering more than 50 varieties such as angelica, codonopsis, rhubarb, astragalus, pinellia, wolfberry, licorice, and Cynomorium. More than 200 varieties of Chinese patent medicines have been imported from Lanzhou Foci Pharmaceutical and Gansu Meierkang Pharmaceuticals, and more than 50 conventional varieties have been maintained.**

**However, with the development of Chinese herbal medicines in Gansu Province, the quality control of Chinese herbal medicines is also particularly important. Like food safety issues, the safety of Chinese herbal medicines is also particularly important in people's minds. In the process of collecting and processing Chinese medicinal materials, problems such as counterfeit and shoddy products and expired products have arisen. This system uses the characteristics of non-tampering and re-encryption in the blockchain to design a relatively complete Chinese medicinal material management system.**

**Keywords：Blockchain；Asymmetric encryption**

# 一、绪论

现存的中药产业供应链存在着信息不及时，无法保证真实性已经可被篡改和删除的缺点。区块链技术中的不可窜改以及加密技术可以比较好的解决这个问题。因此，如何运用好区块链技术于中药材管理，确定其数据的真实性便是现在正在研究的课题。

## 1.1研究背景与意义

### 1.1.1研究背景

在2020年初新冠肺炎疫情肆虐期间,中医有着更深层次的介入。在我国确诊的8万多例中,中医治疗的病例超过7万例,占总数的91% 湖北省90%以上的患者接受过不同程度的中医治疗。中医药防治疫情优势凸显,多种有效方药和中成药得到了广泛应用[1]

看到市场周围存在这些潜在问题，说明中药体系完善、建立流通跟踪体系已经接近尾声。 目前在定西，以大和中华医疗器械等企业为主。 通过采用国际通行的编码技术、条码识别技术、网络通信技术和数据库技术、空间环境、农业技术和高效的采购管理。 部署存储控制以实现强大的控制和信息分析。

区块链作为一种新兴技术，以其去中心化、难以篡改、匿名性和可追溯性等特点，为个性化推荐一同的改进提供了一种崭新的思路。将其利用到甘肃省中医药材管理系统可提高甘肃省中药材管理的严格性，促进甘肃省中医药材的发展。[2]

### 1.1.2研究意义

民以食为天，食以安为先。食品的质量安全理所当然地关系着人民生活的方方面面。党和政府坚持把保障人民群众吃得放心安心放在工作的首位，提出建立食品安全现代化管理体系，旨在运用现代化信息技术来保障食品供应链质量安全。目前国内外在管控农产品质量安全方面都建立了落地的溯源系统，对农产品质量的监控和管理也越来越离不开现代化的农产品溯源系统[3]

本文所研究的基于区块链技术的中医药材管理系统，主要针对于甘肃省中医药材管理系统现存的问题，对药材信息以及加工流程，运输存储信息，以及各种日期等进行了加密设置，防止被篡改和抓包。

区块链技术是关于信息交换思想的全新互联网技术。 秉承他的去中心化、和非寄存、以及联合维护、还有可信的数据库这四大优势，打造甘肃省中药材“从生产到加工、上线”的体系。 溯源系统实现了甘肃中药材从种植、以及加工、流通、销售等全过程的质量信息报送和溯源，以及为现代中药质量溯源与区块链的融合提供了全新基础以及方法和新的手段，以及技术探索新方向、原则。 通过这种新方法、 新技术、新工艺保障了甘肃省中医药材的质量安全，推动了甘肃省中医药材的现代化。 随着区块链技术和中药溯源的发展，中药溯源将更加成熟，中药产业也将带来新的发展和机遇。

## 1.2国内外研究现状与发展趋势

当前区块链技术现状是，国外以区块链基础技术平台或操作系统的研发为主，国内以区块链的应用开发为主。我国企业应用开发主要依赖国外开源社区的成果，尚未出现自主可控的区块链底层架构。根据中国信息通信研究院于2018年10月发布的《可信区块链标准测试情况通报》，有一半的测试厂商使用了IBM主导的超级账本（Hyperledger）区块链底层平台。

同以往的信息技术不同，以规则治理为特征的区块链技术具有很强的扩张性。因此，推动我国区块链技术和产业健康发展的核心目标首先是亟需超前布局自主可控的底层平台和基础技术的自主创新。

### 1.2.1 国内区块链的研究现状和发展趋势

区块链作为点对点网络、密码学、共识机制、智能合约等多种技术的集成系统，提供了一种在不可信网络中进行信息与价值传递交换的可信通道，凭借其独有的信任建立机制，与云计算、大数据、人工智能等新技术、新应用交叉创新，融合演进成为新一代网络基础设施，重构数字经济产业生态。日前，第五届CCF中国区块链技术大会在江苏无锡市举办，聚焦国际区块链前沿创新、发展趋势和关注热点，邀请专家学者、行业大咖、企业精英分享区块链理论创新、技术突破与应用发展，探索建立区块链人才培养体系，合力构建区块链技术与产业发展的新高地。[4]

### 1.2.2 国外区块链的研究现状和发展趋势

国外区块链的论文最早可以追溯到2008年，并从2009年就建立了世界上第一个区块链，但关于区块链技术的学术研究从2013年才算起步，2015年后进入快速发展阶段，呈爆发式发展趋势。

从研究的国家看，美国在研究数量上位列第一，截至2016年底共有34篇文章；其次是英格兰，共发表11篇文章；其后是德国，发表10篇文章。虽然我国相关研究起步较晚，但也已发表了8篇文章，在亚洲处于领先位置。

在国内高频关键词中，关键词“智能合约”“比特币”“业财融合”和“财务共享”的频次和中心度较高，表明国内研究已经步入区块链2.0时代。相比于国外研究，区块链在会计领域的研究内容以财务共享和业财融合为代表，研究范围较为单一。[5]

## 1.3 本章小结

区块链技术主要体现在产品溯源、数据加密中。将其应用到中药材管理系统中，可以提高系统的可信性以及安全性。为甘肃的中药材提供更好的发展前景。

# 二、 相关技术研究

## 2.1区块链技术：

### 2.1.1区块链的概念

“区块链”一词通常与“分布式账本技术”或 DLT 互换使用，后者指的是使区块链成为可能的底层系统。区块链是一种利用区块存储的链式结构,除了创世区块以外的区块由区块头和区块体两部分组成,区块头存放上一个区块的哈希值(prev block Hash)、随机数(nonce)、Merkle根(Merkle root)等.区块结构[6]

区块链中药溯源系统以区块链层次化模型及区块链中信息不可篡改等特点作为技术支撑，将基本信息及录入的各类信息存储于区块链中，以保障信息真实性、安全性及准确性。同时区块链中药溯源系统针对不同的用户，提供不同的访问查询权限，以在用户可查询到所需信息的情况下，保障信息的安全性。[7]

### 2.1.2区块链的主要特点

(1)透明度

它依赖于记录和共享每笔交易细节的节点网络。 它允许每个人查看交易历史记录或分类帐，从而为您提供完全透明的信息。

透明度在区块链中至关重要，因为它消除了任何怀疑或欺骗的空间。 高度透明系统的性质意味着每一笔交易都将立即得到每个网络成员的验证和授权。 因此，它可以更好地改变企业的运营方式，而不会出现欺诈或机密数据泄露的可能性。

(2)去中心化

由于区块链技术仍然相对较新且不受监管，因此对于那些考虑使用它的人来说，充分理解去中心化概念至关重要。 它是一个点对点系统，这意味着不存在中央机构或服务器。

去中心化数据意味着系统不能被任何个人或团体篡改。 因此，区块链技术比其他存储选项更安全。

(3) 不变性：

区块链包含并验证数据的有效性，以使信息不可更改。 此外，该技术非常安全，消除了伪造的可能性，这意味着对记录或数据的任何更改都会立即显示出来。 最后，它使区块链成为一项非常可靠的技术，因为没有数据丢失或损坏的机会。

如果没有网络上每个参与者的同意，也不可能逆转或更改交易。 它在系统中的所有参与者之间提供了一定程度的独立性和安全性以及信任元素。 这些功能在处理合同和管理供应链中的买卖流程方面提供了优于现有系统的独特优势。

(4) 分布式

区块链是分布式的，这意味着节点分布在多台计算机上，创建了一个每个人都可以访问相同信息的网络。 这意味着数据验证系统分散在所有参与者中，并且可以被公司以各种方式使用。

区块链技术是开源的，这使其成为希望降低成本和提高效率的企业的强大工具。企业可以负担得起转向区块链技术以改善其供应链管理系统并进一步降低成本。

(6) 互操作性

互操作性是指不同方或组织通过公共数据库或数据库系统轻松地相互通信的能力。 它是任何系统的重要方面，使公司能够发送和接收有关其业务的实时信息。 例如，智能合约可以有一个用例来在网络上的买卖双方之间发送订单或付款。

无需在区块链系统中手动输入数据，因为智能合约允许无延迟地执行业务流程。 与大多数计算机系统一样，这使得以最少的人工干预记录交易变得非常简单。

(7) 更快的结算

由于许多商业交易的时间敏感性，交易速度是区块链最重要的属性之一。 例如，企业必须及时结算合同、销售产品和支付员工工资，而区块链技术可以确保这一过程尽可能快。

对于涉及跨境和国际交易的企业来说，一个可以促进这些交易的解决方案将非常有用，因为他们可能无法立即获得资金或其他形式的支付。 它使公司在其供应链管理系统中解决国际贸易时使用区块链技术非常方便。 区块链技术提供的成本节约是巨大的。

## 2.2加密算法

加密算法是区块链技术的核心。正确的选择加密算法，并且将其应用到系统中，可以最大程度上避免信息被修改。

本文使用了NodeJS来完成前后端的所有开发。

区块链中主流的4种共识算法分别是工作证明（PoW）、权威证明（PoA）、权益证明（PoS）和经过时间证明（PoET），但实际应用中，只有PoW和PoA共识算法存在大量应用场景[8]

### 2.2.1 NodeJs和crypto

Nodejs框架是基于V8的引擎，是目前速度最快的Javascript引擎。

crypto加密模组，是NodeJs中的第三方模组。

Crypto库是随Nodejs内核一起打包发布的，主要提供了加密、解密、签名、验证等功能。Crypto利用OpenSSL库来实现它的加密技术，它提供OpenSSL中的一系列哈希方法，包括hmac、cipher、decipher、签名和验证等方法的封装。

### 2.2.1 非对称加密技术

非对称加密需要两个密钥：公钥和私钥。 公钥和私钥是一对。 如果数据是用公钥加密的，那么只能用对应的私钥解密。 如果数据是用私钥加密的，那么只能用对应的公钥解密。 由于加密和解密使用不同的密钥，所以称为非对称加密。

RSA算法是一种非对称加密算法,也是目前最有影响力的公钥加密算法。在RSA公开密钥密码体制中包含一组密钥对,即公钥和私钥,公钥对外公开,而私钥是私密的,由用户保管[8]

非对称加密算法的健壮性比较复杂，其安全性取决于算法和密钥。 但由于算法复杂，加解密速度不如对称加密。 在对称加密系统中，只有一把钥匙，而且是不公开的。 如果你想解密它，你必须将密钥传达给对方。 所以保护它就是保护密钥，非对称密钥系统有两个密钥，其中一个是公开的，所以不需要像对称密码那样传输另一个的密钥。 因此，安全性要大得多。

### 2.2.2 哈希加密算法

哈希算法并不是一个特定的算法而是一类算法的统称。哈希算法也叫散列算法，一般来说满足这样的关系：f(data)=key，输入任意长度的data数据，经过哈希算法处理后输出一个定长的数据key。同时这个过程是不可逆的，无法由key逆推出data。

如果是一个data数据集，经过哈希算法处理后得到key的数据集，然后将keys与原始数据进行一一映射就得到了一个哈希表。一般来说哈希表M符合M[key]=data这种形式。

哈希表的好处是当原始数据较大时，我们可以用哈希算法处理得到定长的哈希值key，那么这个key相对原始数据要小得多。我们就可以用这个较小的数据集来做索引，达到快速查找的目的。

## 2.3 本章小结

RSA算法本身很简单, 关键是选择正确的密钥。这是一个高强度非对称系统, 密钥长度至少为500位, 一般为1024位, 这就使得加密的计算量非常大, RSA算法能够抵抗到目前为止已知的所有密码攻击, 是目前最有影响力的公钥加密算法。对于网上的大量用户, RSA可以将加密密钥以文件的方式储存起来, 解决了大量网络用户密钥管理的难题, 这是公钥密码系统相对于对称密码系统最突出的优点。[9]

通过在后端加密传输，在前端解密显示的方式，完全把解密步骤嵌入到客户端里，把加密步骤放在后端里，这样网络中传输的只是密文，避免了修改的危险。

# 三、系统需求分析

## 3.1 功能性描述

本系统将用户划分为消费者、生产者和管理员（监管者）。

（1）消费者：消费者需要注册和登录来生成私钥和公钥。并且将生成的公钥发送到后端数据库。消费者在登陆之后，需要输入自己购买的药材名。便可以查询到有关此药材的操作流程和相关信息。

（2）生产者：生产者注册账户之后，同消费者一样，会生成自己的私钥和公钥。但是需要发送给后端数据，所以需要获取到后端发来的公钥并保存到本地。生产者需要把自己负责的药材信息上传到系统。并且根据真实情况上传药材生产加工步骤。

（3）管理员：主要负责管理员账户和用户账户的增删查改，并且可以直接更改用户的公钥，以及核对生产者上传的数据的合法性。保证系统的顺利运行。

### 3.1.1 在区块链网络中分布、持久的存储药材信息

区块链网络每一个区块都分为两部分，一部分是块头，存储着上一个区块的哈希值，一部分存储着data，例如药材的名称，数量，以及收购时间，售价进价，还有其在生产线上的每一步操作都是存储在区块链里面。

其去中心化保证了数据的可靠性。

### 3.1.2 根据区块链的不可篡改性溯源

管理员登陆后台管理系统之后，可以查看所有药材的信息，以及每一种药材所在的块信息。例如每一个块的块头，区块体。因为其块头存储着通过哈希算法得到的上一个块的哈希值，所以如果一个区块链中的数据被改变，则会出现错误，区块链网络会自动诊断错误并且回溯。所以区块链的存储方式也决定了其不可篡改的特性。

### 3.1.3 通过操作区块链网路中的块操作药材信息

每当管理员增加了一种药材信息或者生产者上传、修改药材信息时，系统采用哈希加密算法拿到最前面一个块的哈希值，然后将数据用非对称加密算法得出的密文添加到此块体中，并且将新加的一个块加入到区块链网络中，通过共识机制让其他分布式节点认可此区块。至此完成了在整个区块链网络中新增一种药材信息的操作。

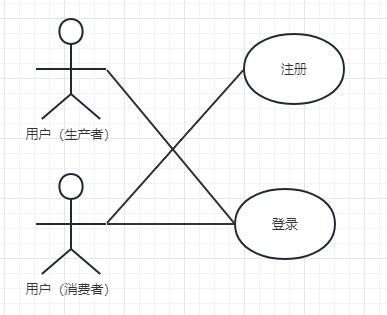
## 3.2 用例规约描述

通过对以上的系统使用场景进行分析可以归纳为以下点：

（1）用户（生产者消费者）登陆注册

系统允许消费者自行注册，不允许生产者注册。生产者想要使用本系统的话需要提交申请到管理员，管理员审核通过之后方可使用。

系统的登陆注册需求模型如图1所示。其用例描述如表1所示。



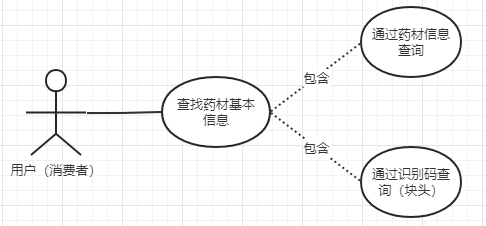
**图1 用户登录注册用例图**

|  |  |
| --- | --- |
| 用例名称 | 用户登录注册 |
| 用例ID | 001 |
| 操作者 | 属于本系统的消费者和生产者 |
| 用例说明 | 用户想使用本系统需登陆注册验证身份后方能使用 |
| 前置条件 | 用户登陆的身份信息存在数据库中 |
| 基本操作 | 消费者可以直接进行登陆注册，生产者必须等待注册申请通过后方能登录 |
| 系统响应 | 如正确登录则跳转到系统首页，如登陆失败则给出错误提示 |
| 异常事件流 | 输入格式有误时会给出错误提示 |
| 后置条件 | 用户可以正常使用本系统 |

**表1 用户登陆注册用例描述表**

（2）消费者通过各种信息查询区块来查找药材信息（溯源）

消费者想通过区块链网络进行溯源操作时，可以在系统的搜索页面提交自己购买的药材信息进行溯源。其用例图如图2所示。其用例表如表2所示



**图2 消费者溯源操作用例图**

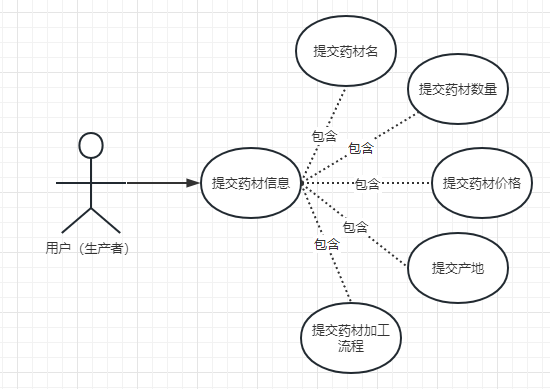
|  |  |
| --- | --- |
| 用例名称 | 用户查询药材信息（溯源） |
| 用例ID | 002 |
| 操作者 | 属于本系统的消费者 |
| 用例说明 | 消费者想通过区块链查询信息 |
| 前置条件 | 用户已经登录到本系统且查询的药材存在于区块链 |
| 基本操作 | 消费者通过输入自己购买的药材信息或者其唯一的标识码 |
| 系统响应 | 如果系统在区块链网络中查找到对应的块则返回药材信息和其一系列的操作。如查询不到则返回空 |
| 异常事件流 | 输入不符合规范时会报错 |
| 后置条件 | 系统通过用户输入的信息返回对应的药材信息或者空信息 |

**表2 消费者溯源操作用例表**

（3）生产者在区块链网络中新增区块来新增药材信息

生产者想要提交自己生产的药材并加入区块链网络，需要提交自己药材的基本信息，并且等待管理员审核后方可加入到区块链网络（上链）

其用例图如图3所示，用例表如表3所示



**图3 生产者提交药材信息（上链）用例图**

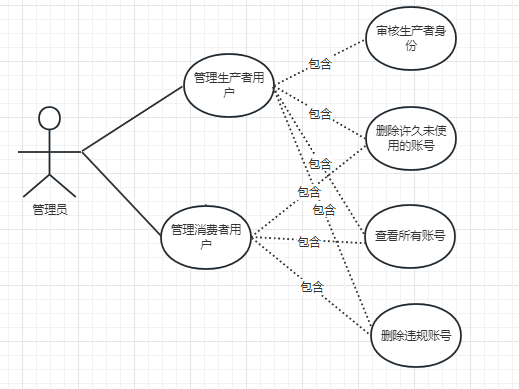
|  |  |
| --- | --- |
| 用例名称 | 生产者新增药材信息（上链） |
| 用例ID | 003 |
| 操作者 | 属于本系统的生产者 |
| 用例说明 | 生产则想通过新增区块链块来新增药材信息 |
| 前置条件 | 生产者已经登录到本系统且通过系统验证了身份 |
| 基本操作 | 生产者提交药材信息和加工流程等基本操作等待管理员审核 |
| 系统响应 | 系统将生产者提供的信息提交给管理员审核，回审核结果 |
| 异常事件流 | 提交的药材信息不符合规范时会报错 |
| 后置条件 | 系统返回管理员审核的结果，如审核通过则成功上链，审核失败则不允许上链 |

**表3 生产者提交药材信息（上链）用例表**

（4）管理员管理用户的基本信息

管理员同时也是监管者，对系统种的用户包括生产者和消费者进行管理。

其用例图如图4所示，用例表如表4所示



**图4 管理员管理用户用例图**

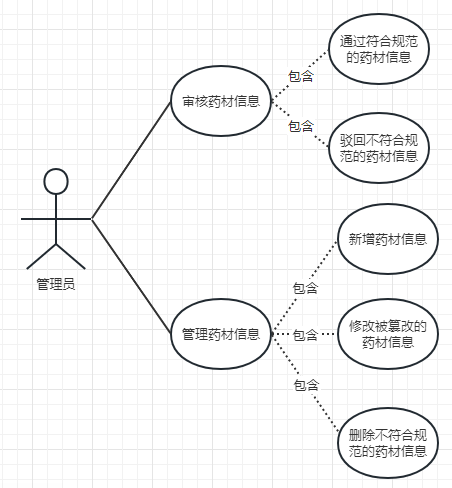
|  |  |
| --- | --- |
| 用例名称 | 管理员管理用户信息（上链） |
| 用例ID | 004 |
| 操作者 | 属于本系统的管理员 |
| 用例说明 | 管理员对使用本系统的用户账号进行管理 |
| 前置条件 | 管理员登录了管理员身份的账号 |
| 基本操作 | 管理员对生产者账号进行审核，以及回收那些太久未使用的用户账号，还可查看所有账号 |
| 系统响应 | 系统返回管理员的操作结果，返回全部账号的信息 |
| 异常事件流 | 管理员审核通过不正常的生产者账号则发出警告 |
| 后置条件 | 管理员审核通过的生产者账号可以进行上传等操作 |

**表4 管理员管理用户用例表**

（5）管理员管理药材区块信息

管理员定期检测区块中是否有区块被更改，也要审核生产者上传上来的药材信息是否合规。如果有发现被篡改的区块或者不合规范的药材信息，要及时删除。

其用例图如图5所示。用例表如表5所示。



**图5 管理员管理药材区块信息用例图**

|  |  |
| --- | --- |
| 用例名称 | 管理员管理药材区块信息 |
| 用例ID | 005 |
| 操作者 | 属于本系统的管理员 |
| 用例说明 | 管理员对使用本系统的药材区块信息进行管理 |
| 前置条件 | 管理员登录了管理员身份的账号 |
| 基本操作 | 审核需要上传的信息，修改和删除不符合规范或错误的药材信息 |
| 系统响应 | 系统返回管理员的操作结果 |
| 异常事件流 | 管理员审核通过不正常的药材区块信息则发出警告 |
| 后置条件 | 审核通过则可以上链，反之被删除 |

**表5 管理员管理药材区块信息用例图**

## 3.3 非功能性描述

(1) 系统易用性：系统需要界面简洁，图标需要能够表达出功能的需要。主要功能不能隐藏的太深，方便用户查找。

(2) 兼容性：由于目前环境各种设备层出不穷，系统需要兼容移动端，网页端，以及桌面端。移动端需要做好不同操作系统的适配和稳定性。网页端需要做好不同浏览器的适配和兼容性。

(3) 隐私权：需要保证用户的隐私性。在网络传输数据的时候。把带有用户数据的cook和token的信息必须做加密传输。可以利用不可逆的md5算法做加密

(4) 可靠度：系统需要保证用户的信任，保证系统的可靠性，不会出现数据丢失，数据造假等问题。

## 3.4 本章小结

本章通过对系统用户分析，产生三个用户身份，分别是生产者消费者和管理者。从这三个身份出发，衍生出几个重要的系统功能。最后从系统的易用性、兼容性分析，还要保证用户的隐私和系统的可靠性。

# 四、 系统设计

## 4.1 系统设计的原则与目标

本系统是基于区块链的中医药材管理系统，旨在高效，安全的管理甘肃省的中医药材，促进甘肃省中医药材的集中发展。该系统在设计之初遵循以下几大设计原则和设计目标：

### 4.1.1系统设计的原则

（1）稳定性：系统稳定性很重要，即使以实施为代价。 虽然灵活性不是很大，但是维持系统的稳定性还是很有必要的。 虽然它有一个不友好的用户界面，但系统应该不稳定。 有时系统设计没有优化以方便系统扩展，有时系统不够稳定以实现高性能。 如何选择和平衡不同的需求 不同的架构师会做出不同的决定。 但我认为一致性是最重要的。 无论设计多么先进和灵活，无论电源多么强大，如果不稳定，请不要在没有适当测试的情况下打开它。

（2）可扩展性：一个先进的管理系统具有很强的可扩展性和灵活性，因为今天的业务需要快速变化，如果每一个小的变化都会导致大量的系统变化，这样的结构是失败的。 因此，架构师必须积极应对未来的变化，设计出灵活、可扩展的架构。

（3）用户友好性：设计须要以人用为本，最终要为人之所用。 系统设计和结构设计不相同。 界面设计不是动态的，而软件设计要以人为中心，更多为用户行为和体验考虑。

### **4.1.2 系统设计目标**

（1）实现以区块链的方式存储信息，实现药材信息的持久化，分布式存储和不可篡改性。实现智能合约和分布式账本。

（2）设计简洁的操作界面，较简单的操作流程，界面要符合各种设备需要。设计小程序以增加用户友好性。

（3）分模块开发，每个功能保证可以独立运行。减少系统出错时的损失。

（4）保证数据的安全。实时备份系统的数据。保证用户信息的安全。

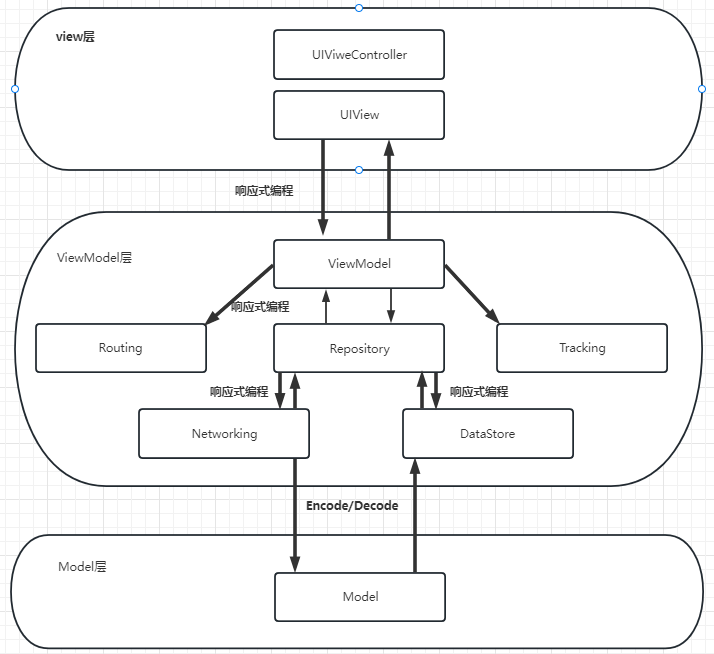
## 4.2 总体架构设计

系统总体采用前后端分离的开发方式。采用MVVM的设计模式。

VVM是Model-View-ViewModel的缩写，是一种常用的前端设计模式。 它是MVC模式（Model-View-Controller）的一种变体，由于MVC模式的controller逻辑更多，协调度更高，所以分为两部分。 MVC模型。

在MVVM中，View层是用户界面，ViewModel层是负责处理数据和逻辑的模块，Model层是数据模型。 具体而言，View 层中的控件连接到 ViewModel 层中的数据，ViewModel 层捕获用户输入和逻辑，并更新 View 层中的数据。

其基本结构如图6所示。



**图6 MVVM设计模式示意图**

（1）后端服务器采用NodeJs+Express框架搭建后端服务器。

（2）数据库采用mysql数据库，利用可视化工具Navicate辅助开发

（3）前端后台管理系统采用React+Antd-Design+React-router-dom设计架构，用户端采用Vue3框架+Vant3组件库设计。小程序端使用微信小程序开发设计。

## 4.3 系统功能设计

根据系统的功能需求，本系统主要有用户登录注册模块，管理者查询修改信息模块

，消费者查询模块，生产者上传信息模块。

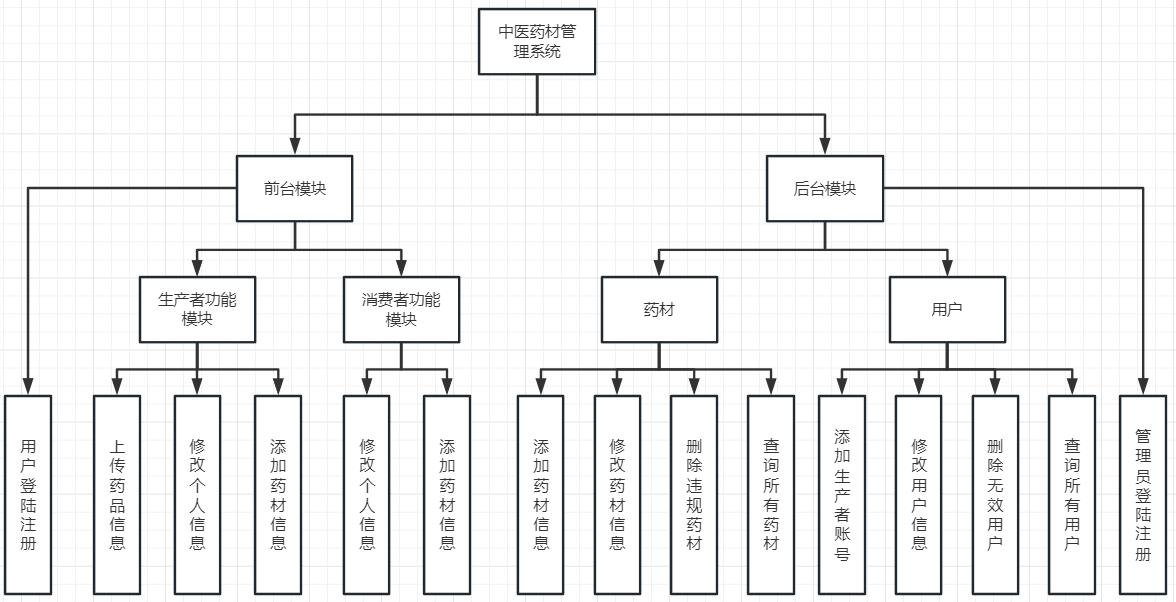
（1）用户登录注册模块：用户通过登陆注册拿到系统的公钥，并且将自身生成的公钥返回到系统数据库。然后将生成的私钥存到本地用来解密。

（2）管理员查询修改模块：管理员可以查询药材信息和用户账户信息并审核。后端将数据用公钥加密之后，前端用私钥解密然后渲染。

（3）生产者上传信息模块：生产者将数据按照实际情况给输入到系统，系统通过登录返回的公钥加密数据后传输到后端处理。

（4）消费者查询模块：用户通过客户端查找购买的药材名，后端通过登录生成的公钥加密数据后，传输客户端，客户端通过本地生成的私钥解密后展现到页面上。

系统的功能模块图如图7所示。

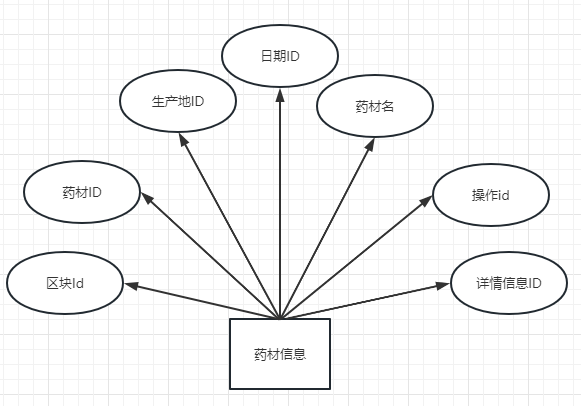


**图7 系统功能模块图**

## 4.4 数据库设计

### 4.4.1 药材信息表

药材信息表存储了药材表ID,生产地ID,日期表ID，药材名，详细信息表ID等信息。其E-R图如图8所示，其设计表如表6所示。



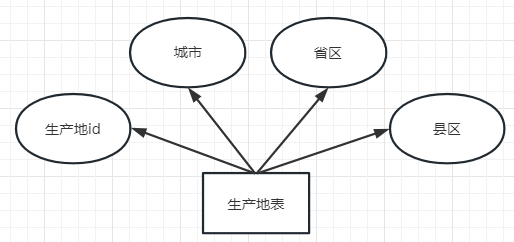
**图8 药材信息表E-R表**

|  |  |  |
| --- | --- | --- |
| 字段 | 类型 | 备注 |
| medicine\_id | int | 药品id |
| grow\_place\_id | int | 生产地id |
| date\_id | int | 日期id |
| operate\_id | int | 操作id |
| name | varchar | 药材姓名 |
| block\_id | id | 区块id |
| detail\_id | id | 详情id |

**表6 药材信息表**

### 4.4.2 药材产地表

药材表包括了生产地ID,省，市，县等信息。其E-R图如图9所示。



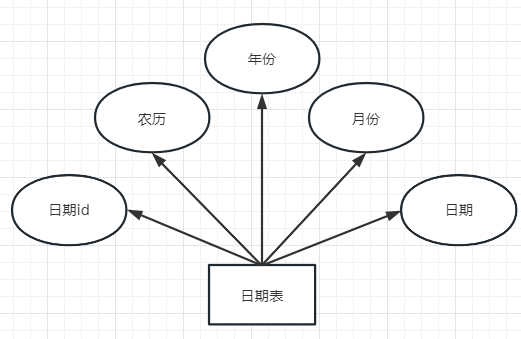
**图9 药材产地表E-R图**

|  |  |  |
| --- | --- | --- |
| 字段 | 类型 | 备注 |
| grow\_place\_id | int | 生产地id |
| city | varchar | 市 |
| province | varchar | 省 |
| country | varchar | 县 |

**表6 药材产地表**

### 4.4.3 生产日期表

生产日期表包含日期id,农历日期，年份，月份，日期字段 其E-R图如图10所示。其设计如表7所示：



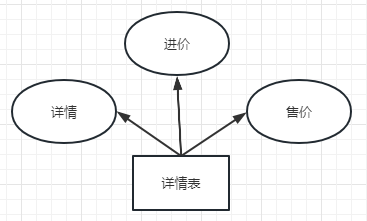
**图10 日期表E-R图**

|  |  |  |
| --- | --- | --- |
| 字段 | 类型 | 备注 |
| data\_id | int | 日期id |
| year | varchar | 年份 |
| month | varchar | 月份 |
| day | varchar | 天 |
| luar\_calendar | varchar | 农历 |

**表7 日期表**

### 4.4.4 药材详情表

药材详情表包含药材详情id,售价，和进价三个字段：其E-R图如图11所示：其设计如表8所示：



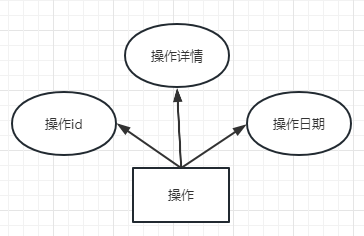
**图11 药材详情表E-R图**

|  |  |  |
| --- | --- | --- |
| 字段 | 类型 | 备注 |
| data\_id | int | 日期id |
| buy\_place | varchar | 进价 |
| sale\_place | varchar | 售价 |

**表8 药材详情表**

### 4.4.5 操作详情表

操作详情表主要包含操作id,操作详情，操作日期三个字段，其E-R图如图12所示。其设计如表9所示



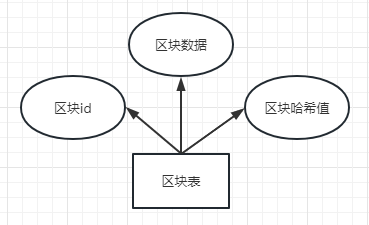
**图12 操作详情表E-R图**

|  |  |  |
| --- | --- | --- |
| 字段 | 类型 | 备注 |
| operate\_id | int | 操作id |
| operate\_detail | varchar | 操作详情 |
| operate\_date | varchar | 操作日期 |

**表9 操作详情表**

### 4.4.6 区块表

一个区块中有区块id,区块hash值，区块data三个字段，其E-R图如图13所示：其设计如表10所示



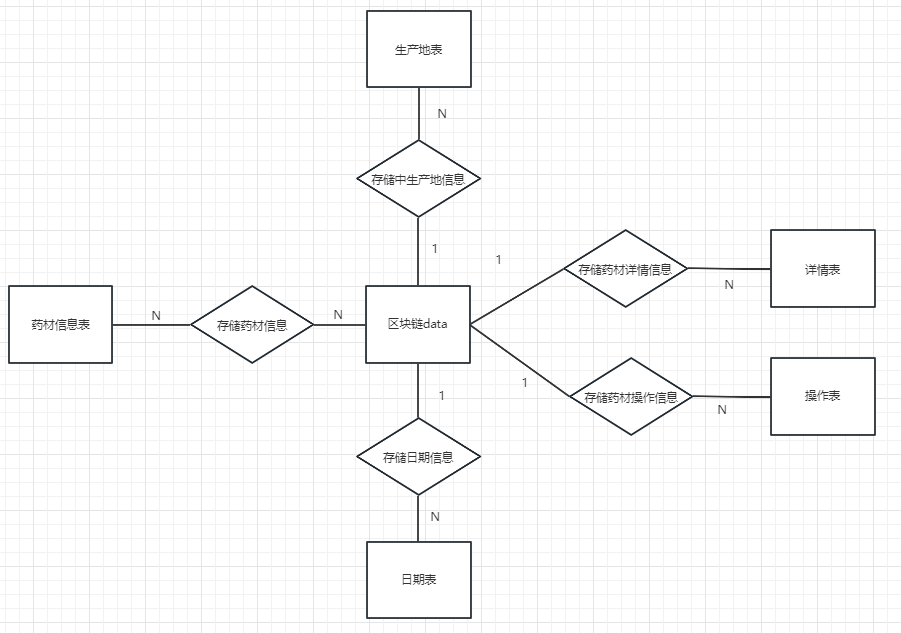
**图13 区块表E-R图**

|  |  |  |
| --- | --- | --- |
| 字段 | 类型 | 备注 |
| block\_id | int | 操作id |
| block \_data | varchar | 区块数据 |
| block \_hash | varchar | 区块哈希 |

**表10区块表**

### 4.4.7总体E-R图

系统总体E-R图如13所示



**图13 系统总体E-R图**

## 4.5 本章小结

本章按照系统设计目标和原则，对整个系统进行层次化设计，系统各层相对独立，然后根据系统功能需要，将系统分为不同的模块，然后进行了数据库设计，将数据存储在区块链上。

# 第五章 系统实现

## 5.1 开发流程

### 5.1.1 环境配置

主要环境：NodeJs

React + vite 脚手架搭建本地服务器。React-router处理路由。

通过npm下载crypto库实现非对称加密算法

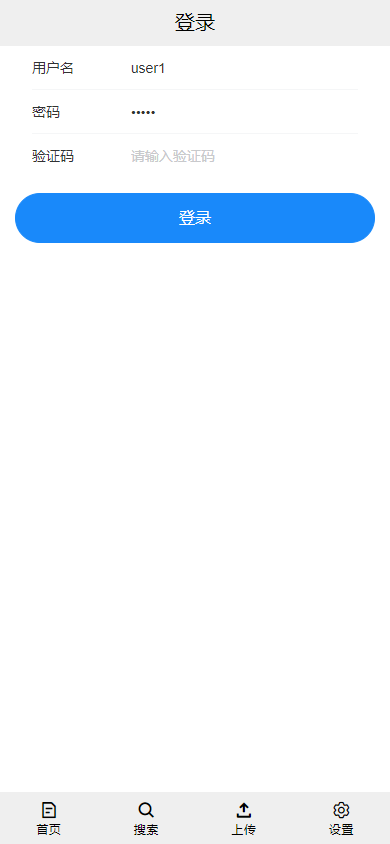
## 5.2功能实现

## 5.2.1 管理员和用户登陆注册实现

进入系统首页之后，会查询本地有无登录状态信息。如果有则跳转到系统首页，如果没有则跳转到登录界面登录。管理员不允许注册，只允许系统管理者新增。



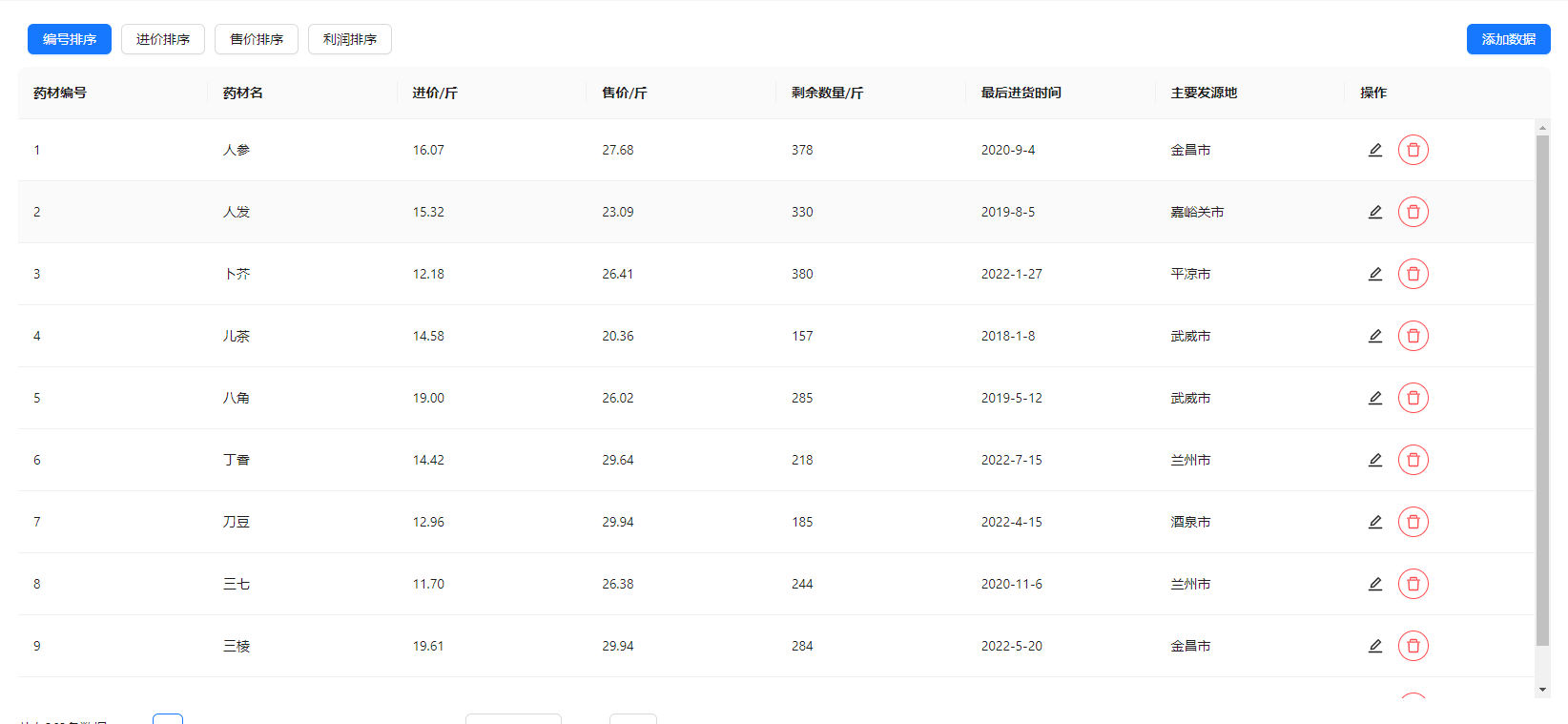
**图四 后台管理系统登陆界面**



**图五 用户登陆界面**

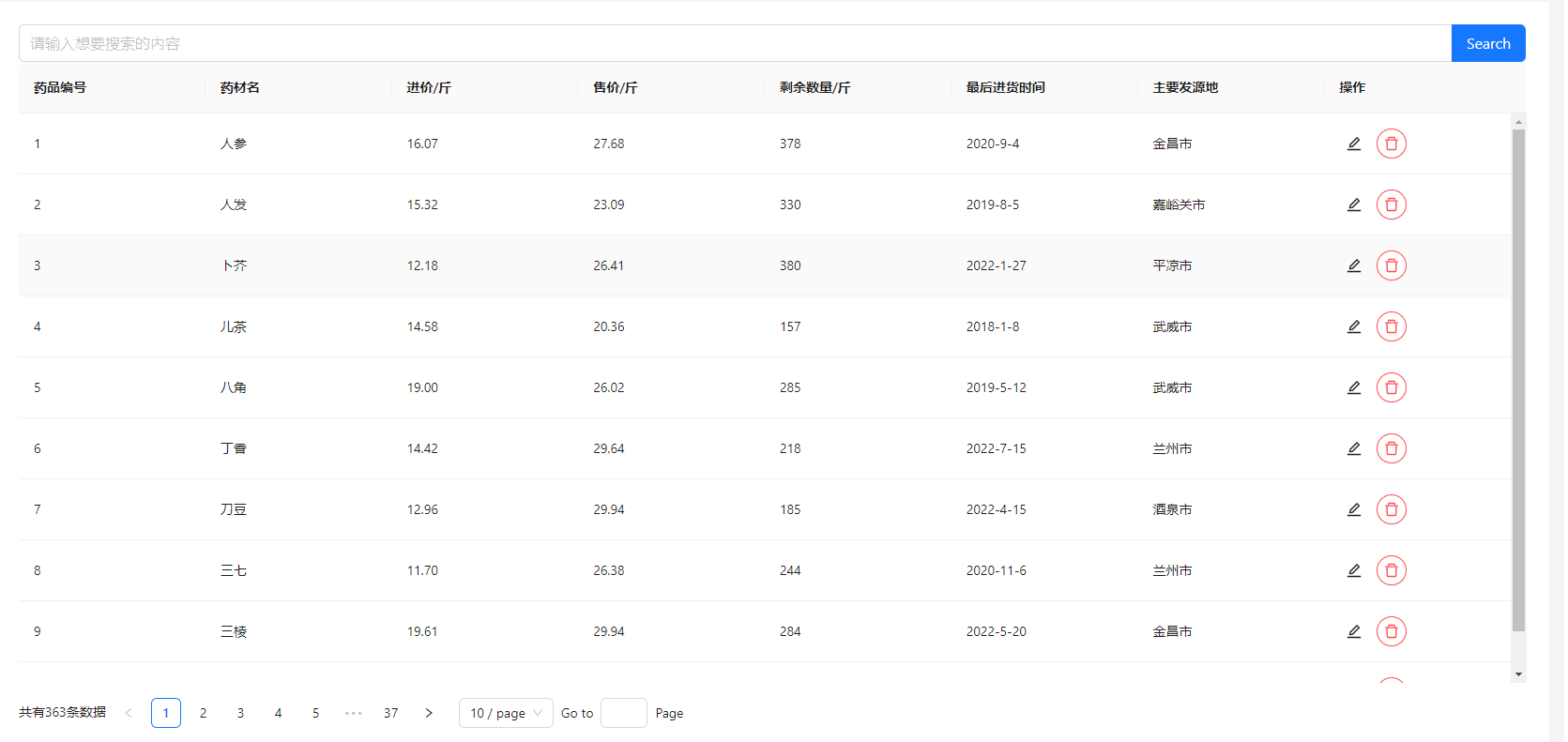
### 5.2.2 管理员查询和搜索功能实现

管理员可以查询所有的药材信息，并且查看某个药材详情。管理员还可以模糊查询药材信息，并查看药材详情。



**图六 查询所有药材信息界面**



**图七 药材详情界面**

**图八 搜索药材信息界面**

### 5.2.3 修改数据功能实现

管理员可以修改不符合实际的药材信息。



**图九 管理员修改药材信息界面**

### 5.2.4消费者查询和搜索功能实现

消费者根据产地、药材名等可以查询此药材从种植到出售所有的步骤



**图十 消费者搜随界面**



**图十一 消费者查看药材详情界面**

### 5.2.4 生产者上传数据功能实现

生产者可以根据真实情况提交自己的药材，监管者会在后台审核



**图十二 生产者上传药材信息**

## 5.3 本章小结

本文实现了基于区块链的中药材管理系统的基本功能。首先介绍了系统开发所需要的环境搭建，以及数据库设计，后端和前端同时实现了加密算法。

系统总共实现了管理者增删改查，以及用户查询和生产者查询的功能。

# 第六章 系统测试

## 6.1系统功能测试

（1）用户登录注册模块

**表一 用户注册登录测试**

|  |  |  |
| --- | --- | --- |
| 测试数据 | 预期结果 | 测试结果 |
| 输入无效用户名密码是否可以登录 | 无法登录且报错 | 无法登录 |
| 不登录是否可以直接跳转到页面 | 无法跳转到页面 | 无法跳转到页面且跳转到登录页 |
| 密码强度不够是否可以注册 | 不可以注册 | 不可注册 |
| 是否自行注册生产者账号 | 不可注册 | 不可注册 |

**表二 用管理员查询修改测试**

（2）管理员查询修改模块

|  |  |  |
| --- | --- | --- |
| 测试数据 | 预期结果 | 测试结果 |
| 模糊查询是否能搜索 | 能查询到结果 | 能查询到结果 |
| 修改数据时格式不合正确是否可以成功 | 不能修改数据 | 不能修改数据 |
| 管理员查询是否可以按需要排序 | 可以按需查询 | 可以按需查询 |
| 是否可以删除数据 | 可以删除数据 | 可以删除数据 |

（3）数据上传模块

**表三 数据上传模块测试**

|  |  |  |
| --- | --- | --- |
| 测试数据 | 预期结果 | 测试结果 |
| 生产者能否成功上传数据 | 可以成功上传 | 可以成功上传 |
| 数据不符合规则是否可以上传 | 不能成功上传 | 不能成功上传 |
| 是否可以上传没有操作步骤的记录 | 不能上传 | 不能上传 |

（4）用户查询模块

**表四 用户查询模块测试**

|  |  |  |
| --- | --- | --- |
| 测试数据 | 预期结果 | 测试结果 |
| 是否可以不登陆查询 | 不可 | 不可 |
| 是否可以模糊查询 | 可以模糊查询 | 可以模糊查询 |
| 是否可以查看详细操作 | 可以查看 | 可以查看 |

## 6.1 本章小结

本章对系统的各种功能进行了测试，使得系统运行更加稳定。证明了系统的可用性。通过不断测试，不同的测试数据都可以通过系统稳定性测试，系统可以正常上线。

# 第七章 总结与展望

## 7.1总结

随着区块链技术的发展，其去中心化、防篡改的特性正好可以解决产业链中不明确流程的问题。中药材因为其分布广阔，无法保证其质量，无法保证在加工运输过程中有无缺斤少两等情况发生。更有甚者利用职权擅自更改系统。因此，接下来的研究主要考虑一下个方面：

（1）介绍了区块链技术的基本特征，使用了非对称加密算法，在一定程度上保证了传输的安全以及数据的安全。

（2）结合前后端分离的开发思想，使用nodeJs搭建后台，React和Vue前端框架分别搭建了前台和后台管理系统

（3）探讨了网络传输中的安全问题，现如今抓包手段众多，不法分子在网络传输中可以通过抓包来制造假的返回数据。如果在网路中使用密文传输，则大大减少了被破解造假的情况。

（4）基于以上，设计实现了基于区块链的甘肃省中药材管理系统，实现各个模块，并进行功能测试。

## 7.2展望

**参考文献**

[1]刘加梦,彭绍亮,李肯立等.基于区块链的中草药质量安全管理模型[J].数据与计算发展前沿,2020,2(05):65-75.

[2] 肖丽,谭星,谢鹏等.基于区块链技术的中药溯源体系研究[J].时珍国医国药,2017,28(11):2762-2764.

[3] 梅育荣.基于区块链的农产品供应链溯源系统的设计与实现[C].南京邮电大学,2021.

[4] 第五届CCF中国区块链技术大会在无锡举办[J].信息网络安全,2023,23(03):104.

[5]王妮,王鹏.国内外“区块链+”会计研究的可视化分析[J].财会月刊,2023,44(04):69-78.DOI:10.19641/j.cnki.42-1290/f.2023.04.009.

[6] 谢春辉,熊蔚维,李国妹等.基于区块链技术的中药材质量安全溯源系统设计[J].云南民族大学学报(自然科学版),2020,29(01):84-90.

[7] 孙赫浓;施明毅.基于区块链技术中药质量溯源系统的设计[J].成都中医药大学学报,2022,(04):95-100.

[8] 王煜,朱明,夏演.非对称加密算法在身份认证中的应用研究[J].计算机技术与发展,2020,30(01):94-98.

[9] 蒋春凤.非对称加密算法[J].内江科技,2012,33(08):148.

[10] 张小波,王慧,郭兰萍等.基于区块链的道地药材高质量发展和认证系统建设探讨.中国中药杂志,2020,45(12):2982-2991.DOI:10.19540/j.cnki.cjcmm.20200416.101.