



**毕业论文(设计)**

|  |  |
| --- | --- |
| **论文题目：** | 基于区块链的中医药材管理系统的设计与实现 |
| **学 院：** | 信息工程学院 |
| **年 级：** | 2019级 |
| **专 业：** | 计算机科学与技术 |
| **学 号：** | 2019051101 |

|  |  |
| --- | --- |
| **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；

**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**

# 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

近年来，甘肃省委省政府高度重视中医药产业发展，加大扶持力度，发挥地域优势，促进中医药产业做大做强。“建立中药材流通追溯体系，从源头上控制药材质量，这不仅能实现标准化种植和管理，还能促进农户增加收入。”兰州佛慈制药有关负责人告诉记者，中药材是药品研制、生产、开发和应用的源头，只有把好源头质量，才能实现中药标准化、现代化生产，才能从根本上保证中药制品的质量。目前佛慈制药公司已与中医学院、兰州大学合作，在漳县、渭源县建立中药材生产基地，建立生产和流通追溯机制，从源头上掌控了药材品质。

对这些潜在的市场流通中显现出来问题，暴露出中药材的流通追溯体系亟待健全，从而形成可监控可追溯的流通体系。目前，在定西市以大河中草药等企业为主，通过运用国际通用的编码技术、条码自动识别技术、网络通信技术和数据库技术等，实现对中药材种子、种苗产地的地理环境、种植过程、采购加工、检验仓储等过程进行有效的动态管理和信息分析。

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。

### 1.1.2研究意义

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。

区块链具有的加密性和不可篡改性，这两种性质正是现存的管理系统急需拥有的。通过区块链技术，打造一个较为安全的药材管理系统，真正实现每一种药材的透明管理。通过甘肃省各地级市的配合，对数据进行整理，促进甘肃省中医药材的发展。

## 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。2019年10月24日，习近平总书记在中央政治局第十八次集体学习时强调“我们要把区块链作为核心技术自主创新的重要突破口，明确主攻方向，加大投入力度，着力攻克一批关键核心技术，加快推动区块链技术和产业创新发展。”区块链是人类历史上首次构建的可信系统，其核心功能是提升各个纬度的治理能力，这也是需要我们深刻理解和准确把握习近平总书记在十九届四中全会之前组织中共中央政治局集体学习区块链的重大意义。

### 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。

从相关文献的类型看(如表1所示)，会议论文有86篇，期刊论文有19篇，工作手稿、新闻条目等占据剩余比例。从文献类型统计结果可知，目前区块链技术在国际上仍处于研究起步期，以会议论文为主，比例约为73.5%。学术会议是交流新思想、新概念、新技术、新方法的合适载体，一些新的理念尚未成熟，不能形成论文或申请专利，但它也很重要，是未来发展的备选方向之一。当然，研究起步期意味着该技术未来主要发展方向尚不明朗，也许会冲击现有的经济、社会体系，如何平衡各方利益尚未有妥善的办法。因此，相关研究应更多关注潜在影响、未来应用场景等问题。

## 1.3 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。

# 第二章 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。 所有参与者（“节点”）都可以访问区块链内交易或账户的共享历史。 这些交易不一定限于汇款或金融工具，还可以包括出生证明和医疗记录等。 除非各方同意（共识），否则任何人都不能更改数据。

### 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。

### 2.2.1NodeJs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 对称加密算法

对称加密算法 是应用较早的加密算法，又称为 共享密钥加密算法。在 对称加密算法 中，使用的密钥只有一个，发送 和 接收 双方都使用这个密钥对数据进行 加密 和 解密。这就要求加密和解密方事先都必须知道加密的密钥。

数据加密过程：在对称加密算法中，数据发送方 将 明文 (原始数据) 和 加密密钥 一起经过特殊 加密处理，生成复杂的 加密密文 进行发送。

数据解密过程：数据接收方 收到密文后，若想读取原数据，则需要使用 加密使用的密钥 及相同算法的 逆算法 对加密的密文进行解密，才能使其恢复成 可读明文。

著作权归作者所有。商业转载请联系作者获得授权，非商业转载请注明出处。

### 2.2.2 非对称加密技术

非对称加密需要两个密钥：公钥 (publickey) 和私钥 (privatekey)。公钥和私钥是一对，如果用公钥对数据加密，那么只能用对应的私钥解密。如果用私钥对数据加密，只能用对应的公钥进行解密。因为加密和解密用的是不同的密钥，所以称为非对称加密。

非对称加密算法的保密性好，它消除了最终用户交换密钥的需要。但是加解密速度要远远慢于对称加密，在某些极端情况下，甚至能比对称加密慢上1000倍。

非对称加密算法强度复杂、安全性依赖于算法与密钥但是由于其算法复杂，而使得加密解密速度没有对称加密解密的速度快。对称密码体制中只有一种密钥，并且是非公开的，如果要解密就得让对方知道密钥。所以保证其安全性就是保证密钥的安全，而非对称密钥体制有两种密钥，其中一个是公开的，这样就可以不需要像对称密码那样传输对方的密钥了。这样安全性就大了很多。

### 2.2.3 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。

稍微想一下就可以发现，既然输入数据不定长，而输出的哈希值却是固定长度的，这意味着哈希值是一个有限集合，而输入数据则可以是无穷多个。那么建立一对一关系明显是不现实的。所以"碰撞"(不同的输入数据对应了相同的哈希值)是必然会发生的，所以一个成熟的哈希算法会有较好的抗冲突性。同时在实现哈希表的结构时也要考虑到哈希冲突的问题。

密码上常用的MD5，SHA都是哈希算法，因为key的长度(相对大家的密码来说)较大所以碰撞空间较大，有比较好的抗碰撞性，所以常常用作密码校验。

## 2.3 小结

区块链中比较重要的方面是加密算法。一个好的加密算法可以保护用户的信息和系统信息，防止恶意抓包修改数据。大大保证了数据的真实性已经系统在用户心中的可信性。

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。

# 第三章 系统分析

## 3.1需求分析

因为本系统是面向甘肃省中药材有关的所有用户。所以主要用户为管理者，中药材生产者和购买者。

### 3.1.1 前台需求分析

前台开发主要面对与中药材消费者和生产者。

(1)对于消费者，消费者需要注册属于自己的账号，生成自己的密钥。并且在输入购买的药材名后，可以溯源到购买的药材的一系列加工流程等。

(2)对于生产者，生产者亦需要注册输入自己的账号，生成自己的密钥。并且在生产药材的过程中，实时提交每一步操作

### 3.1.2 后台需求分析

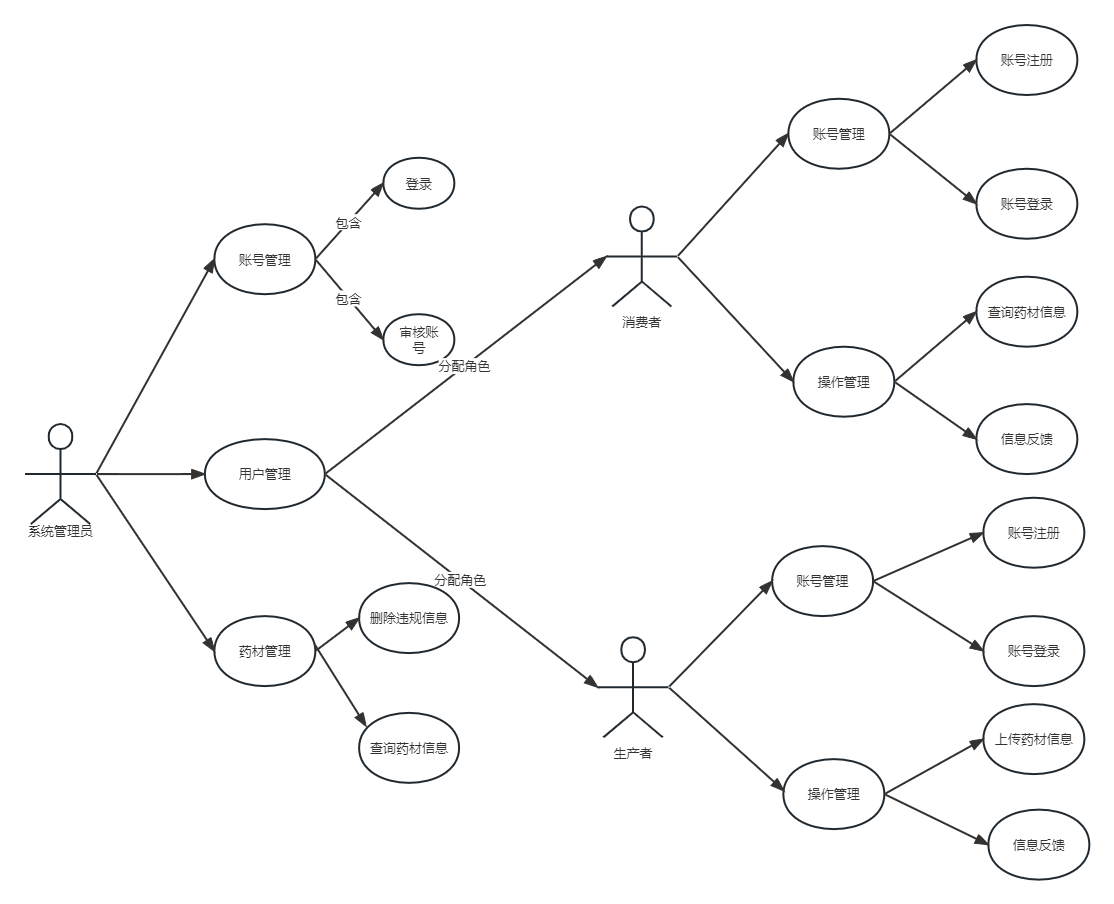
后台开发主要面对管理员（监管者）。管理者需要获取到各个用户的公钥。并且在传输数据时，利用非对称加密算法传输加密后的密文，并且传输管理员本地的公钥。

## 3.2 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品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。

**图1 系统功能用例图**

## 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 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。

# 第四章 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系统设计原则

（1）稳定性：系统的稳定性压倒一切，即使牺牲性能，也要确保系统的稳定。即使扩展性不强，也要保持系统稳定。即使用户界面不友好，也不要系统不稳定。有时候为了实现系统灵活的扩展性，导致系统架构不稳定；也有时候为了实现高性能，导致系统不稳定。如何取舍和平衡，不同的需求，不 同的架构师会做出不同的抉择。但个人认为稳定性放第一位，再先进灵活的框架，再牛的功能，如果不够稳定，坚决不要没有充分测试匆忙上线。

（2）可扩展性：一个先进的系统设计具有很强的可扩展性和灵活性，因为现在的商业需求变化迅速，如果每次小小变化都导致大量系统改动的话，这样的体系结构无疑是失败的。所以架构师必须去主动迎接未来可能的变化，设计灵活的可扩展的架构。

（3）用户友好性：设计以人为本，到头来还是给人用的。可用性设计不等于界面设计。界面设计是静态的，而可用性设计是以用户为中心的交互设计(Interaction Design)，更关注用户的行为和体验。

### 4.1.2 系统设计目标

（1）实现对数据库基本的增删改查等操作。联合查询，模糊查询，

（2）实现简洁的主页界面，人性化的操作流程。

（3）实现非对称算法的密文传输。以及公钥的传输

（4）保证数据的安全。实时备份系统的数据。

## 4.2 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，管理员查询模块

，用户查询模块，数据上传模块，用户查询模块。

（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。

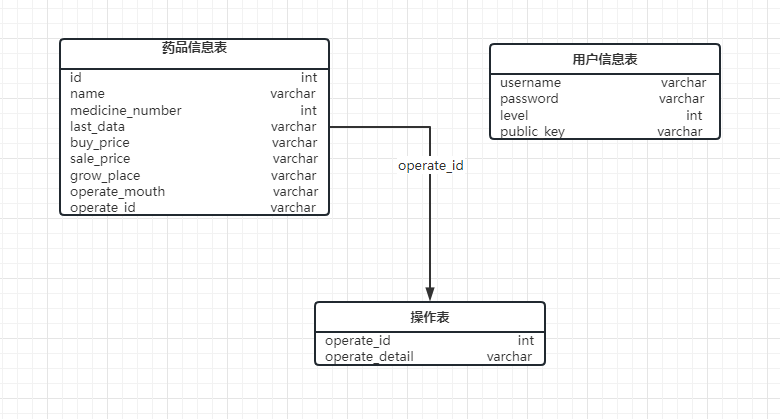
（2）管理员查询模块：管理员可以查询药材信息和用户账户信息并审核。后端将数据用公钥加密之后，前端用私钥解密然后渲染。

（3）数据上传模块：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）用户查询模块：用户通过客户端查找购买的药品名，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。

## 4.3 数据库设计

本系统拥有三个数据库。分别为药品信息表（medicine）,用户表（user）,操作表（operate）。

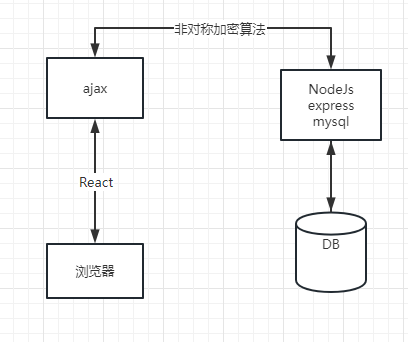


**图2 数据库关联结构图**

## 4.4 总体架构设计

（1）后端采用mysql+NodeJs设计，于3000端口上暴露出api

（2）前端后台采用React+Antd-Design+React-router-dom设计架构，前台采用Vue3+Vant3设计。



**图3 系统架构图**

## 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，通过非对称加密算法处理传输的数据，最后展现到浏览器上。

# 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

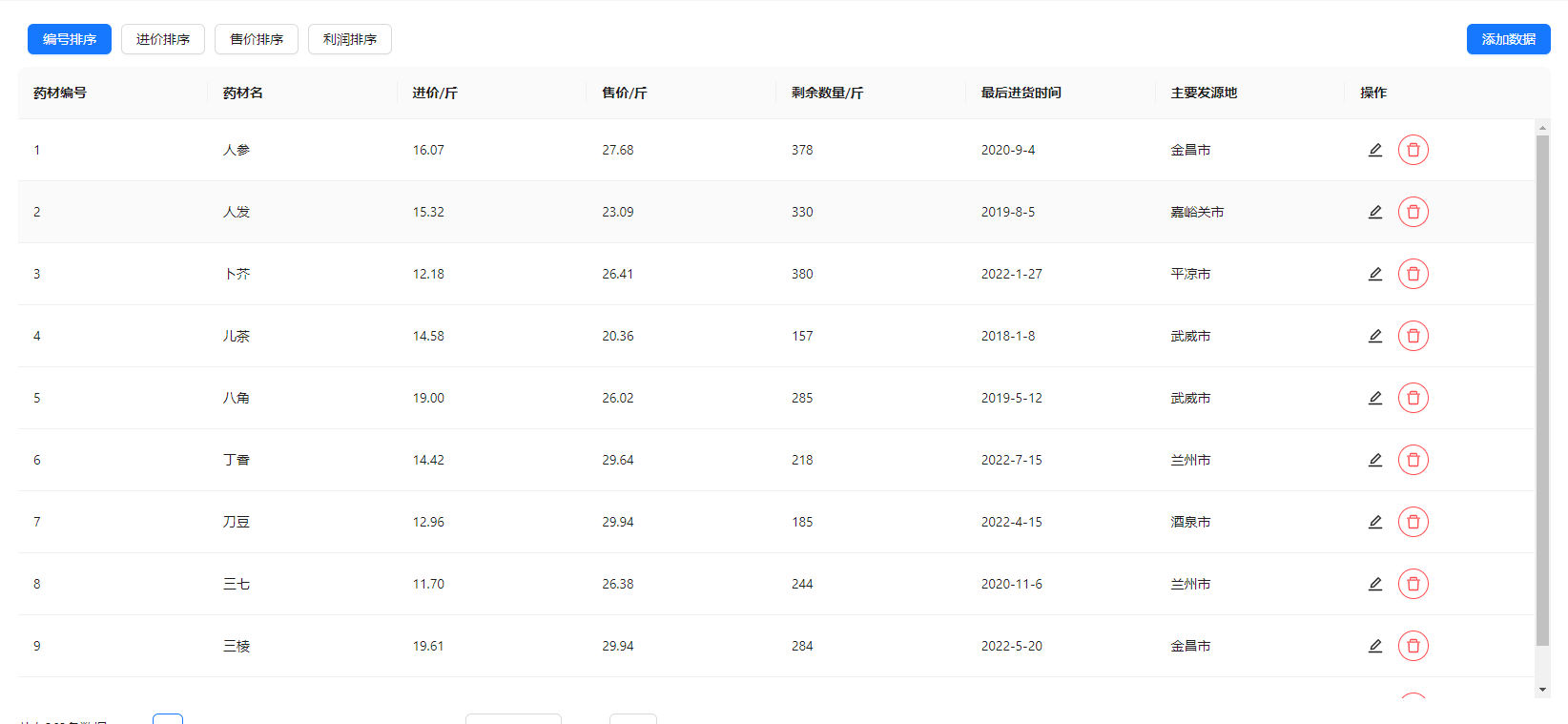
### 5.2.1 管理员和用户登陆注册实现

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。

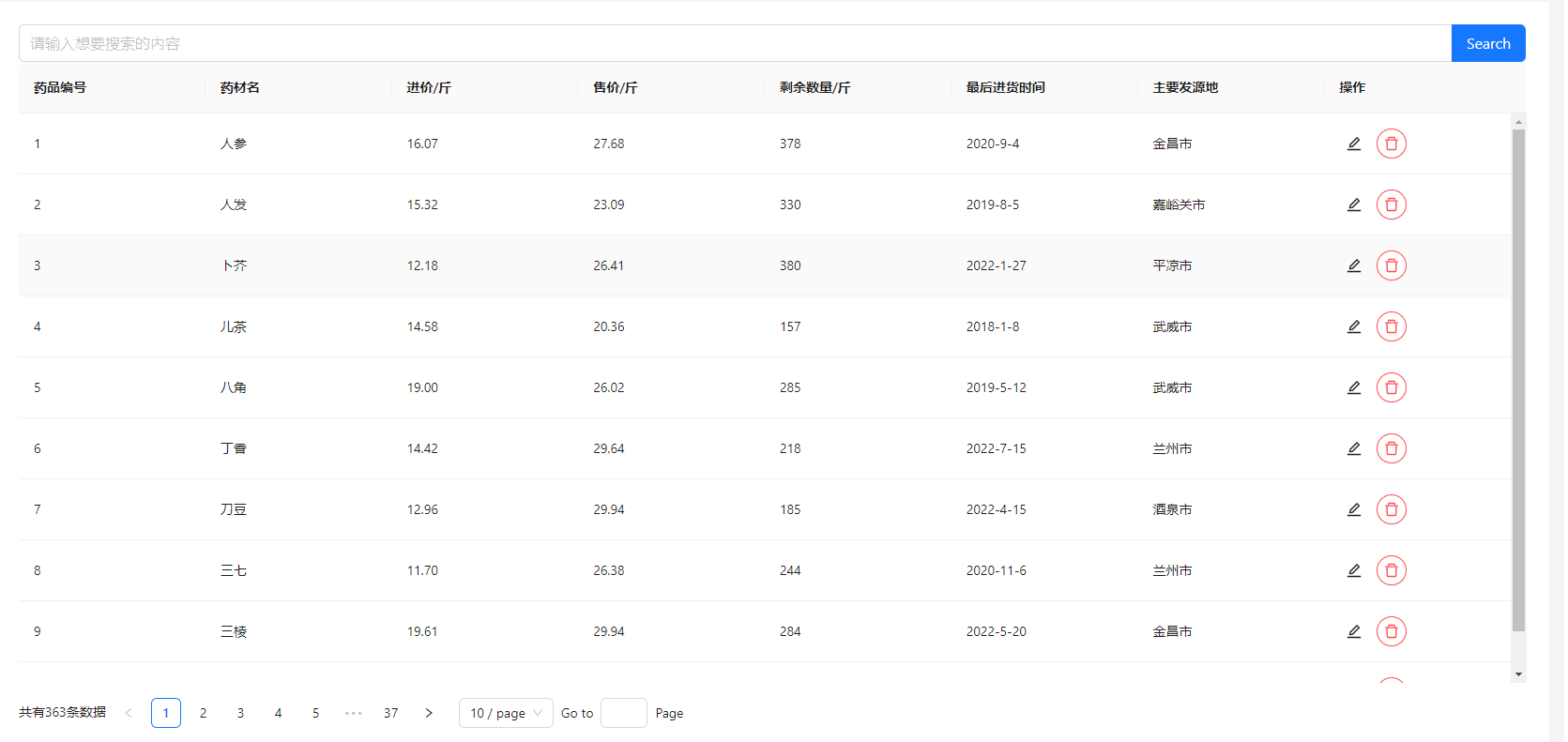


### 5.2.2 管理员查询和搜索功能实现

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品信息，并查看药品详情。







### 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品信息。



### 5.2.4消费者查询和搜索功能实现

### 5.2.4 生产者上传数据功能实现

## 5.3 小结

# 第六章 系统测试

## 6.1系统功能测试

（1）用户登录注册模块

（2）管理员查询模块

（3）数据上传模块

（4）用户查询模块

## 6.1 小结

# 第七章 总结