北京理工大学

本科生毕业设计（论文）开题报告

**学 院：** 计算机学院

**专 业：** 计算机科学与技术

**班 级：** 07111601

**姓 名：** 张峄天

**指导教师：** 张子剑

**校外指导教师：** 方志

二○二零年三月一日

毕业设计（论文）开题报告评审表

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 姓名 | | 张峄天 | | 学号 | 1120161675 | 班级 | 07111601 | 专业 | | | 计算机科学与技术 |
| 导师 | | 张子剑 | | 校外导师（职称） | | 方志 | | 校外导师单位 | |  | |
| 论文选题 | 题目名称 | | | 基于区块链的供应链管理系统的设计与实现 | | | | | | | |
| 题目性质 | | | 软件开发（ ） 理论研究（ ）  工程设计（ √ ） 技术科学研究与工程技术研究（ ） | | | | | | | |
| 题目来源 | | | 结合科研 （ ） 结合生产实际（ √ ）  结合实验室建设（ ） 自拟题目 （ ） | | | | | | | |
| 评审组成员 | 姓 名 | | | 职 称 | | 工作单位及职务 | | | 签 字 | | |
|  | | |  | |  | | |  | | |
|  | | |  | |  | | |  | | |
|  | | |  | |  | | |  | | |
| 评  审  意  见 | （含：选题意义；选题是否满足毕业要求；技术方案是否可行；进度安排是否合理等） | | | | | | | | | | |
| 成 绩 | | |  | | | | | | | | |
| 评审组长签字： 年 月 日 | | | | | | | | | | | |

注：成绩以“合格”“不合格”记；评审组长为高级职称人

# 毕业设计（论文）选题的内容

在现代化企业中，供应链是一个保障企业平稳健康运作的关键部分，在现下人工成本和原材料成本都在上涨的情况下，它能帮助企业站在行业全局的角度制定最佳配置策略，并且在市场竞争中取得优势。

供应链是一种单向的网状结构，它展示了包括原料商、制造商、批发商、经销商等从供给侧到需求侧的供应关系，供应链管理的目标是针对这些信息进行计划、调控和优化，使其所耗费的总成本最小。在这个网络中，信任是建立完整的产品制造和销售过程的最大问题，只有解决各个商家之间的相互信任，才能将原本松散的企业构成这种链式结构。其次，供应链包含了信息流、物流和资金流三种流动过程，物流从供给侧指向需求侧，资金流从需求侧指向供给侧，而信息流则需要在各个商家之间共享。目前，供应链现状是这三种流动过程各自独立运行，这种模式存在信息流作假、数据整合难、产品追踪能力弱等缺陷。区块链技术的诞生恰好解决供应链管理面临的难题，首先区块链提供的去信任性能够帮助供应链上下游的商家低成本地构建起供应链关系，其次区块链的信息公开透明、节点间对等以及不可篡改等特性能够帮助供应链管理实现信息流、物流和资金流的三流合一，打造更高效可靠的供应链管理模型。

本课题深入分析与研究上述供应链中存在的问题，结合现有区块链技术，尝试设计并实现一种基本的供应链管理溯源系统，构建简单的金融系统，解决商家之间的信任和供应链数据整合。以此为基础，完成毕业论文，详细介绍该系统的设计思路，通过原型系统进行功能展示。

# 研究方案

* 1. 本选题的主要任务

1、了解供应链管理中的基本概念，学习区块链技术原理和编程实践；

2、根据供应链中的各个流程和活动，设计针对商家的简易供应链管理系统；

3、设计供应链上下游的商家和用户端App，实现三流合一和产品追溯；

4、完成链下与链上系统的联动，并通过原型系统展示各个功能；

5、完成毕业设计论文并提交程序及相关文档。

* 1. 技术方案的分析、选择  
     根据论文阅读，供应链具有以下的特征：供应链结构模式必单个企业的结构模式要复杂；供应链具有明显的动态特征；供应链具有面向用户需求的特征；供应链具备一定的交叉特性。影响供应链的因素有很多[1]。

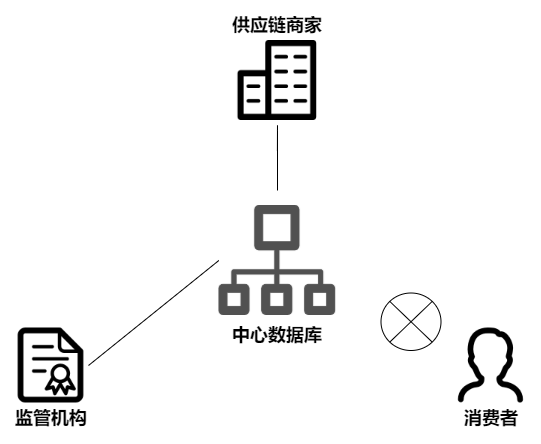
通过调查学习，我了解到目前大部分企业的供应链管理模式仍然采用的是独立运行、分散管理的模式[1]，采用传统的数据库模式进行数据存储，由各商家派遣各自的技术人员进行数据记录、存储、管理和维护工作，数据仅在商家之间流通，消费者则无从知晓产品所处供应链的具体情况，如图1所示。这种模式存在信息流易作假、数据整合困难、产品供应链信息追踪能力低下等明显的缺陷[6]。

图 1 旧式供应链管理模式

区块链技术的诞生能够为目前供应链管理的尴尬境地提供一个较好的解决方案。基于区块链平台，我们可以构建新型的供应链管理体系，如图2所示。

首先区块链提供的去信任性能够帮助供应链上下游的商家低成本的建立起供应链关系；其次，区块链的信息公开透明、节点间对等以及不可篡改等特性能够帮助供应链管理实现数据流通的统一,打造更高效可靠的供应链管理模型[1][6][8]。

图 2 新型的供应链管理体系

我们可以通过以下几点对比来体现区块链方式相较于传统的供应链信息管理技术的优点：

|  |  |
| --- | --- |
| 传统方式 | 区块链 |
| 信息维护困难 | 每个节点都有一份数据副本，去中心化，即使某一节点的数据损坏或失效，也不会影响整体的数据安全性和完整性。 |
| 信息流易作假 | 当需要向链上写入数据/完成一笔交易时，都需要通过背书策略完成共识后才能进行，使得数据的写入得到多方认同，较之传统方式更加保证了数据来源的真实性。 |
| 信息易篡改 | 信息通过附加的方式写入链中，一旦写入，根据区块链的原理可知，想要篡改数据基本上是不可能的。 |
| 数据整合困难 | 通过制定规范的数据写入标准，将数据写入链上后，通过链码可以定位特定产品的所有供应链信息。 |
| 链上供应商难以建立信任 | 区块链提供的去信任性能够帮助供应链上下游的商家降低成本地构建起供应链关系。 |
| 信息不能公开透明 | 区块链可以提供信息查询，并且节点对等以及不可篡改等特性能够确认信息的真实性。 |
| 消费者无法对产品进行溯源 | 通过开放API，消费者可以通过易于使用的方式来查询产品的溯源信息，并且这些信息的来源真实可靠，不可篡改。 |

以采用Hyperledger项目作为区块链方案为例，以下几点特性/算法对于供应链的建立提供很大的帮助：

分布式账本：在HyperLedger Fabric中，对于某个区块链网络，其核心可以看作一个分布式账本，在该账本中记录了网络中发生的所有交易信息。区块链账本通常是去中心化的，因为在整个网络中，每个参与者都保存着一个区块链账本的副本，所有参与者通过协作共同维护着账本。这就意味着信息的修改需要供应链的共识，可以在一定程度上保证数据的真实性[2][3]。

除了去中心化与协作，区块链的另一个显著特点是信息只能以“附加”的方式记录在区块链中，同时使用加密技术保障了交易一旦被添加进帐本中，就无法被篡改。区块链的这种不可篡改行让信息来源的确认变得容易，这是由于参与者可以肯定信息一旦写入区块链中几乎不可能被篡改[3]。

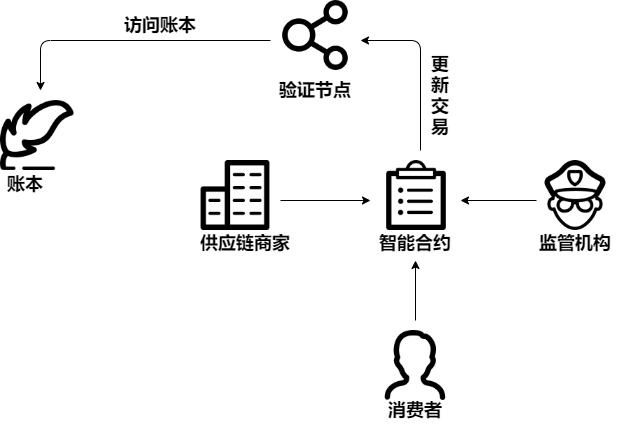
智能合约：为了持续的进行信息更新以及对账本进行管理，引入了智能合约来实现对账本的访问和控制，不仅可以用于在网络中打包信息，也可以被用于自动的执行由参与者定义的特定交易和操作，如图3所示[3]。

图 3 智能合约

共识：共识是保持网络中所有交易的同步流程。共识保障了账本只会在双方都确认后才进行更新。同时在正本更新时，交易双方能够在账本中的相同位置，更新一个相同的交易信息。Hyperledger Fabric的共识机制包括SOLO,Kafka等[3][4][5]。

背书策略：节点通过背书策略来确定一个交易是否被正确背书。当一个peer接受一个交易后，就会调用该交易chaincode相关的实例来确定交易的有效性。为此，一个交易包含一个或多个来自背书节点的背书，校验包括：有效证书签发的有效签名、满足要求的背书数量以及背书需要来自预期的背书节点等。

根据HyperLedger Fabric的种种特性，我们可以选择它作为基于区块链的供应链管理模式的解决方案中后端服务的基础。[2][3][4][8]。

但是相较于传统方式，区块链方式也会有一些较为明显的缺点：

|  |  |
| --- | --- |
| 传统方式 | 区块链 |
| 占用较小的存储方式 | 每个节点都需要保存信息副本，占用较大的存储空间 |
| 信息管理相应速度快 | 上链过程需要产生共识、写入区块等一系列互联操作，响应时间相对于传统方式来说较慢。 |
| 错误信息易于修改 | 如果产生录入错误，则需要对链上信息进行重新上链，并在查询时进行数据清洗。 |
| 便于设置管理、查询权限等 | 需要编写特定的链码进行不同使用角色的权限筛选，较传统数据库方式更加复杂 |
| 有助于保护企业的供应链信息 | 需要对于一些敏感的商业信息做特殊的处理，以免泄露企业的重要商业信息。 |
| 建立成本较低 | 区块链方式需要更高的使用门槛，储存中消耗的空间和时间也更多，对平台的搭建环境有着更高的要求。 |

初步方案：

首先通过前期调查，了解一般企业的标准的供应链模式以及相关信息的种类和形式等具体情况来确定数据的输入、输出、存储格式等问题。

然后使用HyperLedger Fabric搭建区块链平台，对于区块链的数据存储属性，根据上述调查中得出的结论进行调整。

之后，根据供应链信息的流通过程来编写对应的交易链码，包括且不限于信息录入、信息筛选、信息查询等功能，测试之后部署上链。

设计、开放RestFUL API，使得可以通过Web或者其他网络方式对于区块链的链码进行访问，以便于对于数据进行远程管理和访问。

通过界面设计配合网络编程，分别开发面向供应商和消费者等使用群体的客户端，进行链上信息的管理和访问，争取平衡用户的使用体验和系统的整体性能的需求。

最后，整合所有功能，作为原型系统进行使用和相关的测试。在确定系统的稳定性和性能相关数据后，进行展示和答辩。

* 1. 实施技术方案所需的条件

服务后端：云服务器，用于搭建区块链平台，保存节点的安全信息等；

商家客户端：基于Windows平台进行开发和使用，配合Web服务以及二维码扫描工具等。

用户客户端：使用微信小程序等通过扫描商品条码或二维码来进行商品溯源，需要安装有对应操作系统、安装对应APP、并且具有拍摄能力的电子设备。

* 1. 存在的主要问题和技术关键

目前存在的主要问题有如下几个：

1. 区块链技术作为一门新技术，虽然几年来发展速度较快，但是仍然不够成熟，且大部分相关技术仍然只用于数字货币以及金融等领域，专用于进行数据存储和管理的应用并不算多，这意味着可能有许多未知的障碍缺少可参考的解决方案；
2. 即将使用的HyperLedger Fabric项目虽然是一个较大的开源项目，但是版本之间差异较大，并且官方文档完善程度一般，并且在以往的使用经验中，存在许多未知的适配性错误，因此在平台的搭建上可能会遇到比较多的难以解决的问题；
3. 区块链运行对服务器的要求可能会偏高，因此性能限制可能会成为开发过程中的一个问题；
4. 区块链上的信息均是透明的，虽然具有一定的真实性和不可篡改性，但是对于真实的使用场景来说，有许多信息是企业不希望暴露出来的，所以在信息录入和查询时需要对于信息进行有效的规范和筛选，这些标准的制定可能会比较复杂；
5. 链码的编写需要用到Go语言，对于这个编程语言我目前的了解比较少，需要一些时间来学习；

技术关键点：

1. 制定适用于企业供应链应用场景的背书策略。现实场景中，企业的供应链可能交叉程度高，错综复杂，在完整的供应链中，某些交易只需要部分节点的认同即可，所以，制定可行的背书策略，不仅符合现实场景，也能够在某种程度上提升系统的运行效率；
2. 数据的访问级别设置。在真实场景中，供应链上的不同商家以及消费者所能接触到的信息级别不同，企业也希望能够在一定程度上保留自身的商业隐私等不愿意透露的信息，所以，如何在这样一个透明化的信息平台上进行权限的把控，也是一份关键点；
3. 安全透明性与性能的平衡。在数据增多的情况下，虽然我们仍然能够保证数据的安全性、真实性和透明性，但是随着区块的增多和链的增长，是否能够保证平台的使用性能的降低仍然在可以接受的范围内，如何平衡这其中的关系，这需要考虑区块本身的属性设置以及链码相关的算法设计的问题，是系统能否运用于实际生产中的关键点；
4. 设计一种便捷的，能适用于实际情况的信息录入方式，如采用二维码或者条码扫描等方式进行信息的录入，其中的数据转换方式以及录入方式开发也是一个技术要点。
   1. 预期能够达到的研究目标

设计出一种基于区块链平台的基本的供应链管理溯源系统：

能够为整条供应链上的商家以及参与购买等服务的消费者分配相对应的身份标识，并且具有对应的权限。例如，供应商可以写入和查询详细的产品在某个生产部门的数据，而消费者仅能查询该产品的溯源信息，而不能参与信息的新增和修改。

消费者能够对于产品的整个供应链生产过程有大致的了解。消费者可以

构建简单的金融系统，解决商家之间的信任和供应链数据整合。

系统能够稳定运行，运行效率接近现实场景，之后作为原型系统进行使用和展示。

# 课题计划进度表

|  |  |
| --- | --- |
| 1~2周 | 了解供应链的组成和信息流动过程，学习区块链平台的搭建以及链码的编写，撰写开题报告 |
| 3~5周 | 进行前期准备，设计适用于题目需求的区块链平台结构 |
| 5~12周 | 实现该系统，并对系统进行验证和评估 |
| 12~15周 | 完成毕业论文 |
| 16周 | 进行答辩 |

# 参考文献

[1]杨谢雨,王跃兵.我国企业供应链管理的现状及对策浅析[J].民营科技,2016,(10):123. DOI:10.3969/j.issn.1673-4033.2016.10.117.

[2]Hyperleger Fabric项目,https://www.hyperledger.org/

[3]Hyperleger Fabric中文文档, <https://hyperledgercn.github.io/>hyperledgerDocs/

[4]精通比特币（第二版）,Andreas M.Antonopoulos

[5]密码学原理与实践,Douglas R.Stinson

[6]杨谢雨,王跃兵.我国企业供应链管理的现状及对策浅析[J].民营科技,2016,(10):123. DOI:10.3969/j.issn.1673-4033.2016.10.117.

[7]朱建明,付永贵.基于区块链的供应链动态多中心协同认证模型[J].网络与信息安全学报,2016,2(1):00019-1-00019-7. DOI:10.11959/j.issn.2096-109x.2016.00019.

[8] 黄宇翔, 梁志宏, 黄苾, et al. 基于区块链的供应链可信数据管理[J]. 计算机系统应用, 2018, 27(12):11-19.