
# 廣东外語外貿大學

# 本科毕业论文（设计）

题目（中文）去中心化选课系统：

区块链在广外的一种应用模型

（外文）**Decentralized Optional System:**

**A Blockchain Program Model in GDUFS**

姓名（中文）彭博　（拼音）**Peng Bo**

学　　号　20141002561

所在学院　信息科学与技术学院

年级专业　2014 级软件工程专业

指导教师　郑琪　职称　副教授

完成时间　2018　年　3　月　30　日

# 去中心化选课系统：区块链在广外的一种应用模型

彭博 信息科学与技术学院 2014 级 软件工程

**摘　要：**本毕业设计提出了一种基于区块链技术的去中心化选课系统模型，它能演示出学生个体如何通过点对点网络构建出一个公平、有序、安全且稳定的选课系统，中间不需要通过任何统一管理数据和请求的中心化服务器。虽然分布式系统部分达成了以上目标，但是经典的分布模式，依然没有改变"服务器一客户端"的拓扑结构，因此该系统仍然会在负荷超过某个阙值时出现与中心化系统一样的稳定性问题，服务器端也不能有效避免安全性漏洞；其次，分布式系统本身需要更大的开销。该模型将提出一种解决方案，解决选课相关的公平性以及稳定性问题。该网络通过将全部课程所有权请求以区块链的数据结构分布存储，任何一个区块的细节被修改，除非一并修改后续所有区块的工作量证明结果，否则区块链的篡改都会被发现。节点群中存储的最长链即为选课过程中合法选课操作的历史序列记录。除非超过 51%的学生个体节点对全网进行完全一致的攻击，攻击者的链条最终都不会赶超其他诚实节点生成的最长链。这个系统不需要额外投入基础设施，且能够大大削减现有系统的开销。节点可以随时离开和重新加入网络，并将最长的工作量证明链条视为在自身离线期间发生的课程请求记录的证明。

**关键词：**区块链；去中心化；选课系统

# Decentralized Optional System:

# A Blockchain Program Model in GDUFS

Peng bo  School of Information Science and Technonogy

**Abstract:** A blockchain version of decentralized optional system would allow online courses registration be executed directly among only students in a peer-to-peer network without going through a central institution. Distributed system achieve part of the goal, but the main disadvantage of centralized system exists in the model if it is still based on C/S structure. We propose a solution to the stability problem. The network stores course requests by forming record in blockchain that cannot be changed without redoing the following proof-of-work. The longest chain serves as proof of the sequence of course registration witnessed. As long as a majority (over 51%) of students is controlled by nodes that are not cooperating completely in the same pace to attack the network, they will generate the longest chain and attackers' would not outpace. The network itself requires no additional facility structure, with a extra reduction for system in use .Nodes can leave and rejoin the network at any case, accepting the longest chain as record of what happened while they were gone.

**Key words:** Blockchain, Decentralized, Optional System

# 目　录

摘　要：.....I
Abstract:.....II
1　引论.....1
2　预备知识.....1
2.1　广外在用选课系统规则.....1
2.2　区块链基础[1].....2
3　区块体数据结构.....3
3.1 课程所有权.....4
3.2 标准余量根.....4
3.3 广外课程点.....5
4　本系统的工作量证明与难度.....6
5　节点间网络协议规则.....6
6　流程模拟与源码解析.....7
6.1 特殊应对机制——分叉.....11
6.2 特殊应对机制——通缉令机制.....12
7　系统可行性分析.....13
7.1 区块数据的增加.....14
7.2 数据吞吐力.....14
7.3 对现有机制与规则的改善.....15
8　结论.....16
参考文献.....17
致　　谢.....18

# 1. 引论

广外校园网络中的选课系统由学校统一管理维护，但往往在选课阶段当中运作得极其不顺畅，包括部分学生使用非法辅助工具争夺课程以及学校服务器不定期出现宕机等公平性和稳定性问题。学校作为管理总体，不适宜在选课系统中通过硬件资本投入来修正这些问题，同时，软件层面的解决方案也是存在天然短板的。因为选课系统不是长期运作的，如果投入硬件资本会造成很大的资源浪费，而对于大量集中的数据请求，本身软件和硬件层面都不可能完全通过资本投入来完整应对。

所以我们可以结合区块链的技术核心设想这样一种系统模型，它不需要官方机构进行不划算的资本投入，在课程请求处理上依靠密码学原理（以及相关的数学定理）而不是简单的服务器应答来保障安全，它具备区块链保护数据稳定存取和防篡改的特性。通过让学生运行一个微型客户端，在校园网中组成一个点对点网络，每个学生节点之间自动收发数据并进行有规则的加工计算，他们就可以组成一个公平、稳定的去中心化选课系统。学校的服务器资源可以赋闲，也可以在学生资源有不可抗限制时作为普通终端接入该系统的网络参与计算。只要诚实节点计算能力的总和，大于有一直合作的攻击者计算能力的总和，该系统就是安全的。

# 2. 预备知识

## 2.1 广外在用选课系统规则

我们将广外在用选课系统中，学生获得一门课程所有权经过划分为以下过程：

（1） 预选阶段

此阶段是一个不涉及任何竞争问题的登记阶段，学生只需选出想要的课程，假如课程容量不足，将在（2）过程中由学校进行随机抽签定夺。

（2） 抽签阶段

此阶段学校服务器将对学生登记量超过课程容量的课程进行随机抽签，最后幸运者才能得到这门课程的所有权。没有得到所有权的同学可以在（3）过程中进行竞争抢夺，拥有所有权的同学可以在（3）过程中舍弃该课程。

（3） 正选阶段

此阶段学生将在若干日内，自由在选课系统中操作，拥有课程的同学可以选择“退选”， “退选”的课程会即时在系统更新，没有该课程的同学可以对之进行抢夺，一个名额只会有一位同学抢夺得到。

目前在（3）过程中存在最多的公平性问题：

（a）有同学会使用自动化的脚本软件以超过人工的速度抢夺课程，没有脚本软件的同学通过人工的方法几乎不可能胜出。

（b）有同学会在（1）过程中，登记大量课程，在（2）过程抽签完毕后，获得不少自己可能并不需要的课程，即使抛出，也会因为（a）问题导致严重的公平性问题。

（c）学校选课系统服务器，会经常在某些繁忙时间段突发瘫痪，恢复时间极不稳定，让本来存在的（a）（b）问题造成的影响更加复杂化

## 2.2 区块链基础[1]

区块链是一条以一种包含加密处理的数据包－－“区块”，通过首尾相接连结并不断被延长的公开数据链条，每个区块都包含一些公开的基本信息，如与自身连接的上一个区块数据总体的散列值，时间戳，本区块所记录的正文内容。区块链在点对点网络中运作，被设计成具备固有抗篡改的属性，如果想修改一条区块链的数据，必须将该数据之后记录的数据也一并修改，以此类推，并且需要获得网络中大多数节点的认可，否则任意修改都会使链条作废。

### 2.2.1 数据

如果数据依靠简单的键值对直接存储，且需要依靠第三方机构背书保管，则数据的存储会存在安全性隐患。区块链按照时间顺序将键值对数据以状态

转移的格式存储，每一个区块里的数据正文都记载着更早区块中数据最新的状态转移，这样我们只需要通过回溯就可以确定某一个数据是否曾位于某一个状态之中，而不需要担心是否有第三方机构保证它的状态转移过程。

2.2.2 时间戳

区块链节点通过对区块内的数据进行随机散列而加上时间戳，并将该随机散列进行广播。显然，该时间戳能够证实特定数据必然于某特定时间是的确存在的，因为只有在该时刻存在了才能获取相应的随机散列值。每个时间戳应当将前一个时间戳纳入其随机散列值中，每一个随后的时间戳都对之前的一个时间戳进行增强，这样就形成了一个链条。

2.2.3 工作量证明

数据在区块链中仅仅加上时间戳是不够的，区块链根据亚当帕克的哈希现金[2]概念提出了一套工作量证明规则。规则引入了对时间戳散列值的扫描工作，例如，在 SHA-256 随机散列下，要求散列值以若干个 0 开始。随着 0 的要求个数提升，完成这一工作量证明的难度将呈指数级别增长。

节点通过在区块数据尾部增加一个计数位，然后不断尝试直到某个计数恰好使区块散列值达到当前目标要求。区块链网络会根据区块产出速度调整目标难度，使得网络产出区块速度维持在一个稳定值。

2.2.4 网络

区块链在点对点的网络中运行，全体节点通过广播收纳最新数据并制作符合指定工作量证明的合法区块来延长区块链。这些合法区块中的信息就是区块链中合法的信息，与成功制作出此区块的节点无直接联系。

2.2.5 激励

区块链会对区块产出者提供奖励，记录同样和区块中的数据一样纳入区块，以此保证节点积极诚实地维护网络。

## 3. 区块体数据结构

区块总体由区块头、正文和标记位三部分构成。

表 1 区块数据结构

| | |
|---|---|
| 区块头 | 上一区块数据的散列值 |
| | 当前网络难度 |
| | 时间戳 |
| | 标准余量根 |
| | 请求记录散列值 |
| 正文 | 课程所有权请求记录 |
| 标记位 | 随机计数位 |

区块头包含上一区块总体 256 bits 的散列值；当前网络难度为一个 int 值，经过十六进制换算后得出当前产出合格区块所需要对比的标准值；时间戳为标记区块最早生成的时间点；标准余量根是保证相邻产出的区块中，课程所有权对课程余量的修改是连续的，标准余量根与课程所有权的具体描述在本节下文。

## 3.1 课程所有权

我们定义，一位学生经过预选阶段及抽签阶段获得一门课程的所有权表示为“（课程，学号）”的向量形式（如：（a，20141002561），这里我们约定所有课程名在数据底层以字符代号表示以节省存储空间），一位学生在正选阶段舍弃该门课程的所有权表示为“（学号，课程）”的向量形式（如：（20141002561，a）），这些请求只能通过本客户端进行密钥签名后，在点对点网络中广播传送，密钥将在每一次新学期正选阶段前有学校指定并封装与源程序代码中，任何伪造签署、不符通信协议或重放攻击的请求都不会得到广播。进入客户端正常使用必须经过一个广外“学号－密码”的登入操作。

所有在当前区块散列过程中传播的课程所有权请求都直接记录在正文部分，且将正文部分的散列值记录作为头部结构的“请求记录散列值”字段，参与工作量证明计算。

## 3.2 标准余量根

我们定义，自上一区块打包成功后，课程余量完成更新后的结果组成一个向

量值，这个值按顺序陈列各门课程当前最新的基准余量。所有在新区块计算过程中传播的课程所有权请求，都必须依照该标准值进行校验，只要请求间不互斥，这些请求都将依顺序记入计算中的区块正文，同时实时变更这一基准余量。当某个节点完成区块工作量证明，其他节点也依照区块正文的请求记录，逆向还原区块标准余量根的值，假如该值与它的上一区块的标准余量根值一致，那么就认定，该区块在课程请求校验的环节是按照合法规则进行的。

### 3.3 广外课程点

为了让一个完全去中心化的公有区块链获得持续充足的算力，必须向这一网络加入激励机制。在虚拟数字货币中，成功打包一个货币交易区块的奖励，就是货币本身，激励机制即这一货币系统的价值输入机制，除此之外没有任何价值输入的渠道。如果不加入激励机制，要让互不相干的网络节点去做任何运算都是违反社会学的不可能现象。数字货币运作的成功可以通过数据结构模仿移植到其他应用领域的公有区块链中。

我们约定，区块数据结构正文部分的“课程所有权请求记录”的第一条记录信息，就是一条格式为“（点数，学号）”的记录，这一记录与其他课程请求记录一样被看作一种所有权的转移。

每一个节点在竞争打包最新一个区块的过程中，都会先构造区块基本体，然后加入一条表示定量课程点给予节点自身学号的记录，接下来就会实时记录其他请求数据，一旦有节点打包出合格的区块，那么网络认可之后，也就自然让打包者获得定量课程点这一事实被敲定（此处认为网络已经完成相应的校验步骤）。

最后在区块链数据中可以核算出获得奖励的对应用户学号，我们可以按照需求给点数赋予一些对网络具有正反馈作用的意义。例如，可以规定，获得点数的学号，在新学期选课的预选阶段登记的课程，在抽签阶段可以获得更高的中签率；或者可以规定点数具备一些经济化用途。显然，选课阶段内产生的区块数是恒定的，所以这一奖励的总额也是固定的，这样只要让课程点具备任意形式的价值意义，去中心化系统就具备自行维护的动力，这一动力能促使系统更稳固安全，于是又能促使更多节点愿意去维护。

由此可以认为，给去中心化系统奖励赋予任何形式的价值意义，所需要的价值投入都要比现有系统单纯依赖校方维护所需要的更少，且产生的正面效益更多。

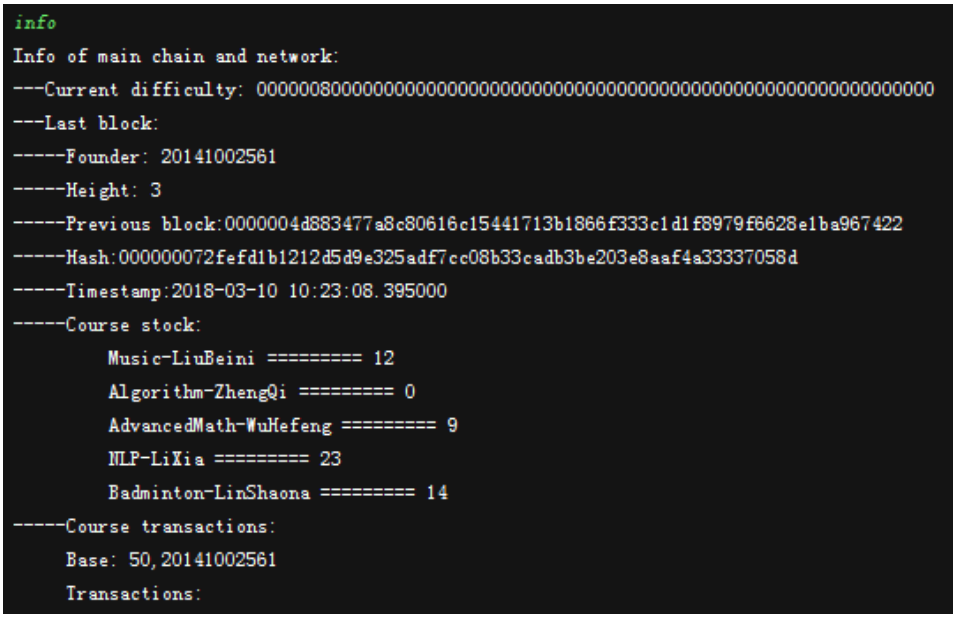


图 1 模型运行中的区块链信息概览

## 4. 本系统的工作量证明与难度

本区块链应用的工作量证明为，对上述数据结构中的头部结构进行指定难度 SHA-256 散列。网络难度将动态调整，如每 12 个区块相隔时间超过 30 分钟，即每个区块平均诞生速率大于 2.5 分钟 / 区块，则网络难度会下调 10%；反之则上调 10%。这个过程在所有网络节点中自动执行，保持一致，在不同网络参与度下维持区块产出速度。

## 5. 节点间网络协议规则

节点客户端的网络模块使用 Twisted[6]框架编程。运行该网络的步骤如下：

（1） 节点通过学号及密码登录客户端，在线的节点互相连接。

（2） 新的课程所有权请求通过客户端向全网进行广播。

（3） 每个节点都将请求添加到一个新区块框架的正文中。

（4） 每个节点在更新区块基本信息后，尝试在自己的区块中完成当前网络需要

的工作量证明。

（5） 必定有一个节点幸运且公平地找到了一个工作量证明，并将新区块向全网进行广播。

（6） 每个节点对新区块进行一系列校验步骤，如果该区块合法，则停止当前自己的工作量证明，将新区块连接到自己的区块链历史数据中。

（7） 全网将会马上开始进行下一个新区块的工作量证明竞争，通过合作延长这条区块链，以表示对这条链上所有历史区块的认可。

节点始终都将存储中最长的链条视为正确的链条，并持续工作和延长它。如果有两个节点同时广播不同版本的新区块，那么其他节点在接收到该区块的时间上必定存在先后差别。他们都会各自在最快到达的区块基础上进行工作，后续到达的区块也会进行保留。等到下一个（或若干个）工作量证明被发现，必有其中的一条链条被证实为是较长的一条（例如长度差距超过若干个区块），那么在另一条分支链条上工作的节点将转换阵营，开始在较长的链条上工作。这一机制的规则将在第六节详述。

如果一个节点没有收到某特定区块，那么该节点会检测到自己的区块链不连续，也就可以提出更新自己区块链副本的请求。

## 6. 流程模拟与源码解析

我们假设一个校园区块链网络中有 Alice（20141009999）、Bob（20141008888）、Charlie（20141007777）和 David（20141006666）四位同学，在各自的设备上使用各自的学号登录了区块链客户端。四位同学的客户端通过点对点网络协议彼此相连，组成一个去中心化的网络，客户端收发的信息都由带有封装的密钥的加密函数签名，保证信息发送者的身份通过了学号验证。以 Python 代码段为例：

```
def make_envelope(msgtype, msg, nodeid):
    msg['nodeid'] = nodeid
    msg['nonce'] = nonce()
    data = json.dumps(msg)
    sign = hmac.new(KEY, data)
```

```
envelope = {'data': msg,
            'sign': sign.hexdigest(),
            'msgtype': msgtype}
return json.dumps(envelope)
```

make_envelope 函数将消息数据进行 HMAC 签名，nonce 字段为防止重放攻击所添加的随机标记。不是通过客户端发送的消息或者非法转发的消息都不会通过验证。

四位同学的客户端内部都包含一个基础区块，在区块链应用中统称为“创世区块”（Genies block）。创世区块的正文内容包括了在抽签阶段中签的同学获得课程的所有权记录;由于其为首个区块,所以“上一个区块散列值”字段为“0”;“标准余量根”则记录抽签结束时所有可选课程最后的余量状况。

区块链所记录的信息是公开透明的，假设现在 Alice 查看记录得知自己获得了 a、b 和 c 三门课程，她希望放弃课程 b，那么她可以在客户端输入“give b”的指令，此时客户端会将一个包含 Alice 请求的数据包广播给其他三位同学。显然，其他同学对照自身的副本数据发现 Alice 确实有这门课程，于是他们都将自己存储的当前“标准余量根”中第二个数值增加 1，表示 b 课程目前余量增加了。假如网络中还有其他同学，他们会将这个正确的请求继续转发出去。

现在全网得知此消息的客户端会将 Alice 的请求记为“20141009999，b”并写入一个空区块的正文部分，包括 Alice 自己。这里 Bob 的客户端中会准备一个如下的区块体：

| 字段 | 值 |
|---|---|
| 上一个区块的散列值 | 创世区块的散列值 |
| 当前网络难度 | 0x80000 |
| 标准余量根 | 12,7,0,6,3 |
| 时间戳 | 当前时间 |
| 请求记录的散列值 | 以下请求记录的散列值 |
| 请求记录 | 50,20141008888<br>20141009999,b |
| 随机计数位 | 0 |

Bob 构造的区块包含的信息与其他三位同学构造的大致相同，除了时间戳，以及第一条请求记录，因为每一个同学接下来都会竞争计算合格区块散列值，所以事先都会为自己添加一条获得“课程点”奖励的请求信息，所有者指向自己。

做完这些步骤后全网的同学都开始了寻找工作量证明的竞争。

```
while KeepHasing == 1:
    if hashlib.sha256(BlockHeader).hexdigest() > 0x80000:
        LuckyNum = LuckyNum + 1
```

此时 Bob 在尝试了将近 2 分钟的时候，发现最新一次的区块散列结果小于当前网络难度 0x80000，于是他马上把这个结果公布给其他三位同学，其他三位同学远没有 Bob 幸运，他们此时仍在计算当中，当接收到 Bob 的消息时，他们对新区块进行了验算，包括：

1、验算区块散列值是否正确且符合当前网络难度

2、检查请求记录中的请求是否来源于历史区块中的数据

3、将正文中的课程请求和标准余量根回滚，检查是否与上一个区块的标准余量根相符

这些检查确保了课程请求是可追溯的，课程余量的变化是连续的。确保了这两点，就可以保证这个区块可以合法地连接到上一个区块的后方了。现在 Bob 获得了 50 个课程点奖励，而 Alice 则舍弃了一门 b 课程。

此时全网节点都更新了自己的区块链副本，副本中顺序记录了 2 个区块，接下来他们都将以第二个区块作为基准，进行第三个区块的竞争计算，过程与上述一致，即使网络中没有任何请求广播，也不影响区块链的计算，节点一样会计算一个正文部分仅包含课程点奖励记录的区块，以保证区块链以一个较为稳定的速度延长，从而防止攻击者伪造区块广播。

如果 Bob 和 Charlie 都希望获得一门课程 c，而此时 c 的余量为 0，那么程

序将允许他们对这门课程进行监听，一旦有同学舍弃此门课程，他们都可以发出指令获取，这一功能抹平了公平性问题（a）中请求方式的不公平因素。

假设此时 David 键入“give c”，请求消息被广播后，Bob 和 Charlie 的客户端就会立刻发出“get c”指令来获取该课程。由于这两个请求是互斥的，网络中其他节点只会承认最快传达的那一个请求，此处我们假定 Bob 和 David 都认为 Bob 最快发出课程请求，Alice 和 Charlie 则认为最快的应该是 Charlie。

此时网络中的节点仍然会继续上面提到过的工作量证明竞争，网络依然认可最快出现的结果。例如 Alice 先于大家计算出了区块的结果，那么所有节点包括 Bob 和 David 都会认可他区块中的内容，也即“Alice 获得 50 个课程点，David 舍弃了一门课程 c，Charlie 获得了一门课程 c”这三条请求，那么 Bob 如果仍然需要课程 c，他将需要继续监听网络。

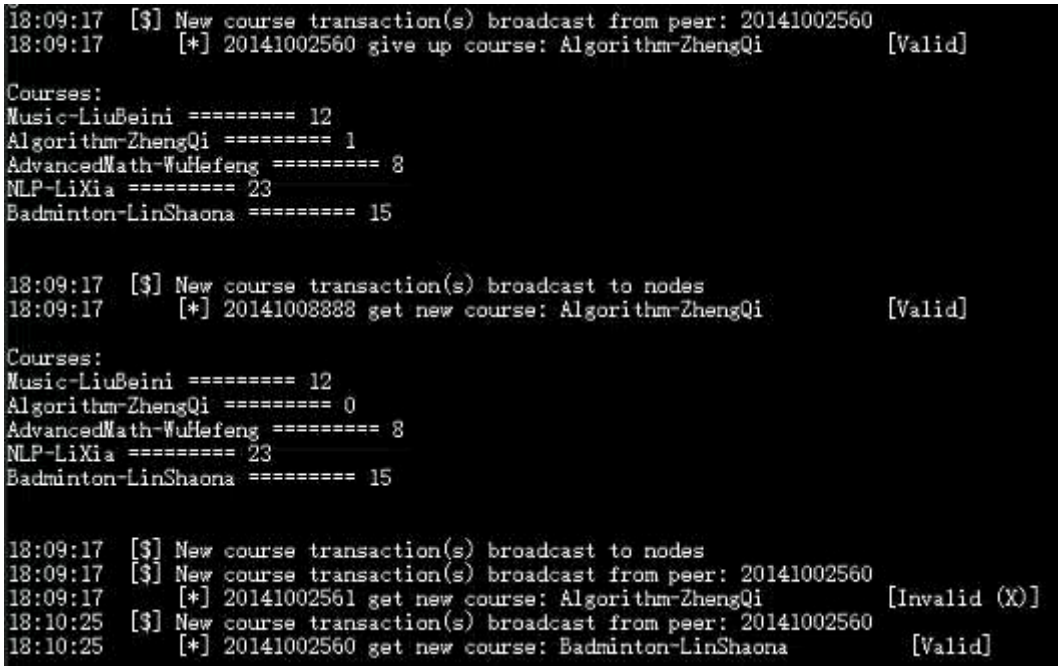


图 2 节点监听课程变化并按照自己观察的先后顺序决断冲突请求

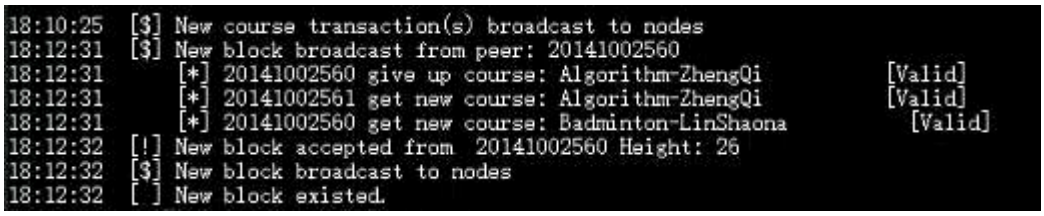


图 3 最快节点的版本胜出，所有不互斥的请求都包含在这个区块正文

## 6.1 特殊应对机制——分叉

上述过程描述的是同一时间出现两个不同请求的情形。假如在区块计算过程中，几乎同一时间出现两个不同的区块，按照网络规则，所有节点除了接纳第一个到达的区块外，还会保留后到达的区块，此时区块链开始一个短暂的分叉。

在工作量证明中，几乎同时出现两个结果的概率极其微小，但如果发生，全网的节点会根据先后顺序分为两派，区块链副本产生分叉。此时全网的算力相当于被分割，所以在两派节点内再次出现分叉的概率近乎为零[4]，所以我们此处只对一次分叉作讨论。

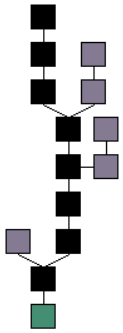

**图 4 区块链分叉概念图**

（资料来源：Bitcoin Wiki）

在产生分叉区块后，全网节点会继续根据自身版本进行计算，相同版本的节点会互相延长，根据理论计算，少数算力者在短时间内赶超多数算力者的概率是快速收敛为零的[3]，也即我们可以在 4 到 5 个区块内，发现其中一个版本的区块链远远超过另一个版本，且数学上能保证可靠性。一旦短链被超越，所有持有短链的节点会将长链部分替换到主链，并刷新数据，此时全网就会回归到统一的区块链版本。分叉的处理与同时请求的处理相似，都仅仅短时牵涉最新区块数据的抉择，对过去发生的数据不会有任何波及。分叉的处理同样是区块链防护伪造链的一个重大模块。

```
10:51:08  [$] New block broadcast from peer: 20141006666
10:51:08  [!] New block accepted from  20141006666 Height: 1
10:51:17  [$] New block broadcast from peer: 20141006666
10:51:17  [!] New block accepted from  20141006666 Height: 2
10:51:36  [$] New block broadcast from peer: 20141006666
10:51:36  [!] New fork block accepted from  20141006666 Forked at: 2
10:51:56  [$] New block broadcast from peer: 20141006666
10:51:56  [!] Fork chain block accepted from  20141006666 Forked at: 2
10:52:10  [$] New block broadcast from peer: 20141006666
10:52:10  [!] Fork chain block accepted from  20141006666 Forked at: 2
10:52:36  [$] New block broadcast from peer: 20141006666
10:52:36  [!] Fork chain block accepted from  20141006666 Forked at: 2
10:52:50  [$] New block broadcast from peer: 20141006666
10:52:50  [!] Fork chain block accepted from  20141006666 Forked at: 2
10:52:50  [!] Fork chain became main chain from  2
```

图 5 构造分叉区块对模型进行分叉测试

## 6.2 特殊应对机制——通缉令机制

假设有某个节点，想通过增加设备而提升计算能力，从而更高效率获取奖励甚至修改副本，本毕业设计提出一个“通缉令机制”可以有效防范此问题。

我们假定上述四位同学的连接拓扑近似链条形，代表网络中可能出现的一种拓扑结构。

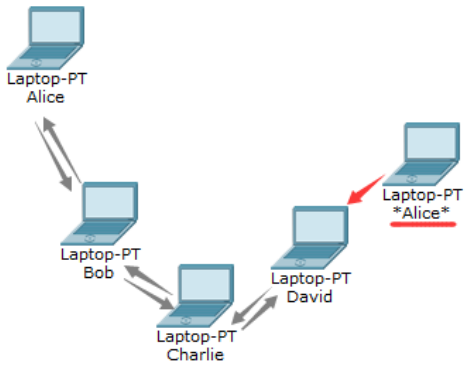


图 6 一种可能被攻击者利用的链形网络拓扑

Alice 发现可以增加一台设备连接到 David 的设备，网络中其他的远端节点并不会发现 Alice 这一举动，从而可以让自己拥有更大的计算能力。

我们规定，所有新节点接入网络的时候，相邻的节点会在全网泛洪一条请求，询问是否有节点连接了此学号不同 ip 地址的节点，假如没有，那么这个节点的连接不会受影响；假如有任何一个节点检查列表发现连接了一个 ip 与请求不一致，但学号却一致的节点，它就会马上泛洪全网，只需要很短时间，就可以让全

网都知道对应学号的犯规行为，并断开与它的连接，作出相应的制裁。

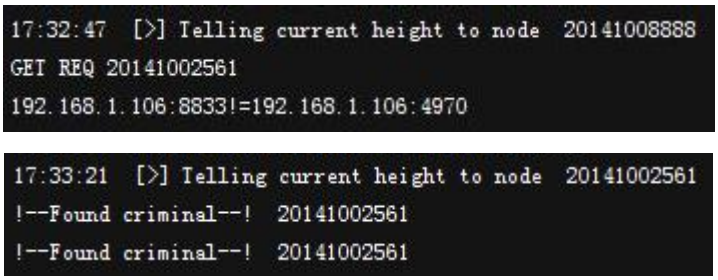


图 7、8 “通缉令机制”下节点间定位犯规者的测试

## 7. 系统可行性分析

上述架构体系在模型实验中可以确保稳定运行，在实际情形中，该模型的实践更可以允许原有的选课系统资源进行赋闲，而不需要额外的资源购置与支出。根据一个调查，近 40%的学生在日间会让个人电脑处于闲置运行，而闲置与使用的总时间均值高达 12 小时，也就是说广外学生在校园网中维护一个区块链网络可行的，况且区块链网络中的节点可以自由选择进出，并且无论节点多少，网络都会动态调整保证区块的产出速度稳定。

而校园网络中还有夜间断网的情形因素，当其时只需要学校将已经赋闲的旧资源在夜间投入运行 6-8 小时，即可保证选课期间区块链网络的稳定运行了，这相对于原来接近 24 小时的运行大有减轻。

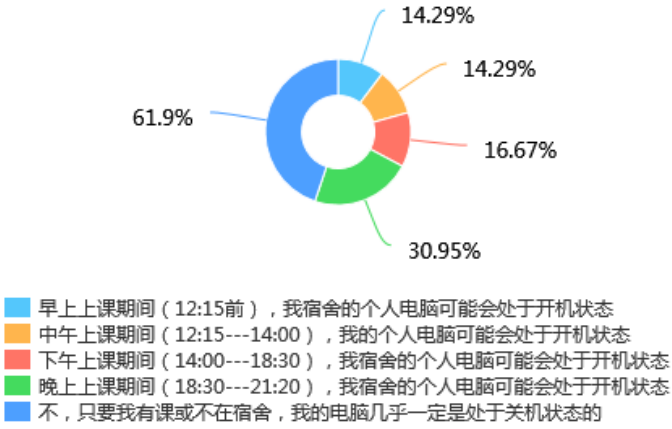


图 9 学生个人电脑日常闲置时间调查（非深蓝色区域有数据交叉）

## 7.1 区块数据的增加

本模型中单个区块体包含 8 个字段，若进行标准工程化后可变为 7 个字段，参考以下数据标准可以估算区块链选课系统数据存储的极限值：

1、全校学生人数约为 40000 人

2、四个年级全专业人均中签课程数为 5 节（不包含学校、学院固定安排的标准课程）

3、选课系统可选课程 60 节

4、区块产出速度为 2.5 分钟/个

5、正选阶段持续时间 12 天，即 288 小时

```
0000000000000000000000000000000000000000000000000000000000000000
0000008000000000000000000000000000000000000000000000000000000000
12,0,9,23,14,12,0,9,23,14,12,0,9,23,14,12,0,9,23,14,12,0,9,23,14,1
2018-02-24 11:12:32.561000
e0cc8e253ddb67a7001c0f31dca29067bdfd3db1ee61fa4ce44416af02467900
50,20141002561 a,20141002561 b,20141002561 c,20141002561 e,201410(
237291683
```

图 10 数据量估算的样例字段

上一区块散列值与当前网络难度值以 64 位字符存储；标准余量根由 60 个整形数以“，”连接组成；时间戳以标准形态存储；课程所有权散列值同第一、二个字段处理；课程所有权间以单个空格连接存储，此处设每个区块都有 5 条不互斥的请求，首条记录为课程点数奖励请求，共 6 条记录；随机计数位按照实际情况以整形数存储；

可估算得，正选阶段区块总量近 7100 个，其中创世区块大小与其余区块大小总和相当，以 TXT 文本为测算载体，各约占 3MB（创世区块估算大小约 2.7MB，余下全链估算大小约 3.69MB），其中单个区块大小在 500B 至数 KB 之间，全链大小预计总和在 6 至 7MB 之间，极限大小不超过 10MB。这个大小的二进制文本对于现阶段的处理器及网络环境来说处于完全可以接受的范围。

## 7.2 数据吞吐力

上文的流程模拟中仅纳入了数条请求记录，实质上在区块未被打包成功期间，所有不互斥的课程请求都可以持续追加（见图 2 最末行消息文本），选课请求只

要是通过验证的，那么就已经可以认为被处理，区块的成功打包则应视为一个提升区块链安全系数的工作量证明结果。

### 7.3 对现有机制与规则的改善

以区块链作为选课系统的载体，有效的解决了文中提到的三个公平性问题，将正选阶段的竞争因素统一到纯粹随机的数学运算中，同时运用数学定理保证竞争以外的安全及性能问题。将原有电力、人力等资源的单纯投入，转化为输出的系统激励，重塑了一个可循环正反馈的网络系统。

我们可以把现有机制中，单个学生正选期间请求争夺一门课程成功的期望表示为 $E(X1)$，那么此概率模型可以归纳为：

$$E(X1) = \sum_{i=1}^{n} x_i p_w \, p_i$$

其中$p_w$为见证概率，也即请求者发出请求前，获知到“此时应即刻行动的信号”之概率。如果一个学生一直不借助任何辅助工具，那么持续尝试的总次数$n$越小，其见证概率收敛为 0，该模型期望值也收敛为 0，提高总次数即代表，加大花费在网页上手动刷新的精力，此时期望值的上升无法弥补人力投入的成本耗费；而当一个学生采用公平性问题（a）中的自动化脚本软件，则等效于不投入人力资源而进行对总次数的高速累加，所以结果会呈现执行时间越长，越能锁定成功率。$p_i$为每一次发出请求成功概率，如果当前网络对于同一节课程的争夺人群中存在自动化脚本软件使用者，那么脚本用户的$p_i$会剧烈压缩其他非脚本用户的$p_i$，也即人群中脚本用户的成功概率上升的同时，非脚本用户的成功概率不但无法上升，还会下降。所有用户在单次争夺中的$p_i$总和小于 1，这是因为包含了学校服务器崩溃停摆的可能性。

我们将区块链方案中的机制期望值表示为 $E(X2)$，则新机制的概率模型可以归纳为：

$$E(X2) = \sum_{i=1}^{n} x_i \frac{N' p_h}{N} \quad (N' \le N)$$

其中本模型的见证概率$p_w$可以理解成恒为 1，因为所有节点都可以对课程余量变化进行监听以抢发请求。真正决定成功概率的包括扩散概率$p_h$，它的变化与

参与争夺的节点数$N'$相关，$N$为在线的节点总数；在$N$中，所有希望参与争夺的节点向周围尽可能快的发出指令，最终所有节点都会根据第一个接收的请求收敛为不同的“派别”，这些派别长期来看是“分布均匀”的，短期来看体现在扩散概率$p_h$是否“幸运的”较大，也即代表请求能不能被更多的节点视为“最先到达者”。分布稳定不再变化后，所有节点就为视工作量证明完成最快的节点所发布的版本为最终结果。

此方案不牵涉节点在见证课程余量变化的速度不公问题，将成功概率关联到，在传播能力一致的情况下覆盖率的竞争问题上，其次覆盖率的竞争仍不是最终竞争，而是需要再结合一次工作量证明中的随机竞争，从而让概率模型中成功概率不会因其他因素影响大幅波动。

## 8. 结论

本毕业设计所提出的一个利用“区块链”的核心技术重塑的广外选课系统模型，采用 Python 语言编程，所有模块均严格跟随区块链理论的标准进行设计，可以直观地对这一模型进行模拟实验，向外界展示其核心规则及原理，从而更客观地探讨其投入实际开发的可行性。

本课题所有内容是作为学生身份进行的个人项目，因此只有资格进行“模型”级别的讨论，所有项目细节都将强调其用于“描述”、“讲解”和“演示”，而非等同“某一项实际措施”的意图。所有机制与规则在本论文提出的假想环境下推导，并可以进行更细致的开发以投入实际应用当中[10]。

# 参考文献：


[1] Nakamoto, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System[J]. Consulted, 2009.

[2] Back, Adam. “Hashcash - a denial of service counter-measure. ” 2002. http://www.hashcash.org/papers/hashcash.pdf.

[3] Feller, William. “An introduction to probability theory and its applications. ” 1957.

[4] Antonopoulos, Andreas M. Mastering Bitcoin. Sebastopol, California: O'Reilly Media, 2014.

[5] Narayanan, Arvind, et al. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton: Princeton University Press, 2016.

[6] Twisted Matrix Labs. Twisted Core Developer Guides. http://twistedmatrix.com/documents/current/core/howto/index.html.

[7] Bitcoin Wiki. Block. 2018. https://en.bitcoin.it/wiki/Block.

[8] Bitcoin Wiki. Bitcoin Core 0.11 (ch 3): Initialization and Startup. 2012. https://en.bitcoin.it/wiki/Bitcoin_Core_0.11_(ch_3):_Initialization_and_Startup.

[9] Bitcoin Wiki. Bitcoin Core 0.11 (ch 4): P2P Network. 2012. https://en.bitcoin.it/wiki/Bitcoin_Core_0.11_(ch_4):_P2P_Network.

[10]刘成. 我国区块链产业有望走在世界前列[N]. 《经济日报》,2017-9-5. http://www.ce.cn/xwzx/gnsz/gdxw/201709/05/t20170905_25734025.shtml.

# 致　　谢

感谢导师郑琪，您对学科领域新概念的开明接纳态度是本论文写就的基石。感谢Satoshi Nakamoto，您首次将区块链概念实体应用化，给后来者以无限的启发。愿区块链技术得到更广泛的认可，怀疑者和反对者终将意识到其宝贵的核心价值。