一、系统介绍

大多数经典密码算法是建立在特定数学难题的基础之上，但是这些数学问题的困难性可能会因新型计算能力或算法的出现而削弱。由于量子计算机在出人意料地快速发展，大量仅能抵御经典计算机暴力破解的密码算法面临被淘汰的困境。尽管主流的密码系统目前依然能够有效运行，但是在量子计算技术的潜在冲击下，几乎所有现有的密码算法都需要改进甚至必须进行迁移。区块链作为当下最热门互联网关键词，拥有着广阔的应用场景，密码学作为区块链的核心技术之一，决定着它的安全命脉。

基于格的密码体制是目前主流的抗量子攻击密码之一，在后量子密码标准化竞争中优势明显。区块链本质是分布式账本，在医疗领域，它最主要的应用是对个人医疗记录的保存，可以理解为区块链上的电子病历，病人的个人数据将不再由第三方机构保管，保证了病人的个人隐私。因此，本软件将目前的区块链中的签名算法替换为高效的格签名算法，即 NTRU 签名算法；而且，本软件中的哈希算法使用基于格的变色龙哈希，在实现区块链可修改性的同时，同时保证区块链具有一定抵抗量子攻击的能力，最终实现基于区块链的医疗信息系统。

二、运行环境

工作平台：Windows 10

高级语言：JavaScript、Python

硬件设备：处理器 Intel Core i5-7200U @ 2.50GHz 2.71GHz；内存 8GB

运行条件：Anaconda3；Python IDE；VSCode；Node.js；

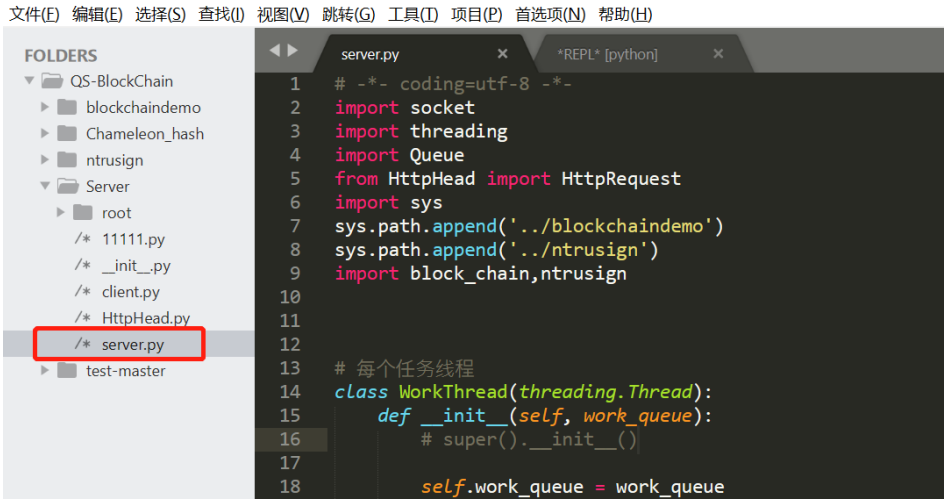
三、实例演示

3.1 准备工作

下载 VSCode 用于运行前端 JavaScript 代码，下载 Sublime 或 Pycharm 用于运行后端 Python 代码，同时下载 Anaconda2 配置 Python 2.7 环境，下载 Node.js 以部署服务器。

3.2 实例演示

首先打开 Sublime 或 Pycharm，并打开整个源代码文件夹，这里以 Sublime 为例，运行主程序 server.py，如下图。



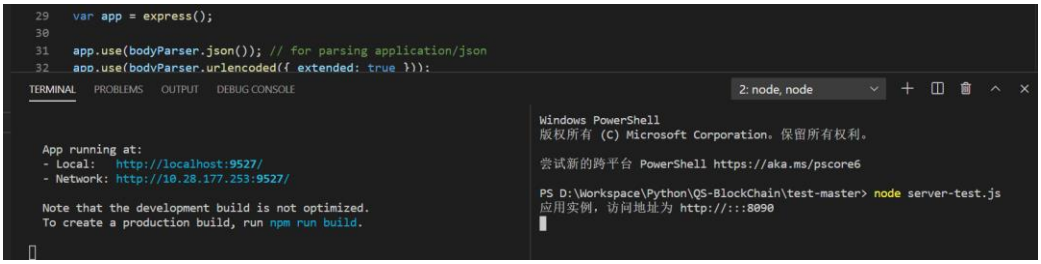
运行主程序将创建创世区块 Genesis Block，并开始监听来自前端的请求，这时将显示创世区块的内容信息，包括序号 Index、上一个区块的哈希 PreHas、当前区块的哈希 CurrHash、数据哈希 Txhash、随机数 Nonce 以及区块数据 Tx，如下图所示。

```
append_block
----------------blockchain begin-----------------
Index: 0
Pre.Has:
Curr.Hash: 06c2e6dc192f1fc1a93e03e2dbff067723e441389d48d66614b35c270dcb52d0
Txhash: [[-4126.]
 [-4345.]]
Timestamp: 1595666059
Nonce:16
Tx:Genesis Block

----------------blockchain end-----------------
listen in 127.0.0.1:9999
```

此时，打开 VSCode，打开 test-master 文件夹，该文件内代码为系统的前端部分，包括所有可视化的 web 界面。

点击上方工具栏的 Terminal，点击 New Terminal，下方将出现命令行终端，在下方命令行输入 npm run dev，加载完成后，将会自动弹出前端 web 页面，点击 Split Terminal（快捷键 ctrl+shift+5）启动另一个终端，随后输入 node server-test.js，启动服务器以进行前后端的交互，此时终端如下图所示。若 web 界面未弹出，可在浏览器 url 地址栏输入 http://localhost:9527/或 http://192.168.1.104:9527/，即可进入登陆界面，点击登录即可进入系统。

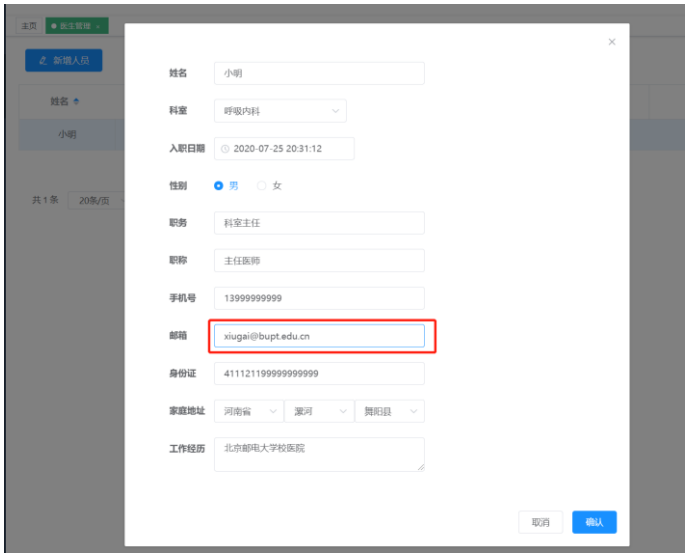


点击左侧导航栏的医生管理按钮，即可进入医生管理界面，如下图所示。

首先演示新增人员功能，假设我们需要新增一位名为“小明”的医生，那么我们点击新增人员按钮，进入信息录入窗口，并填写小明的个人信息，填写完成后点击确认按钮即可，如下图所示。

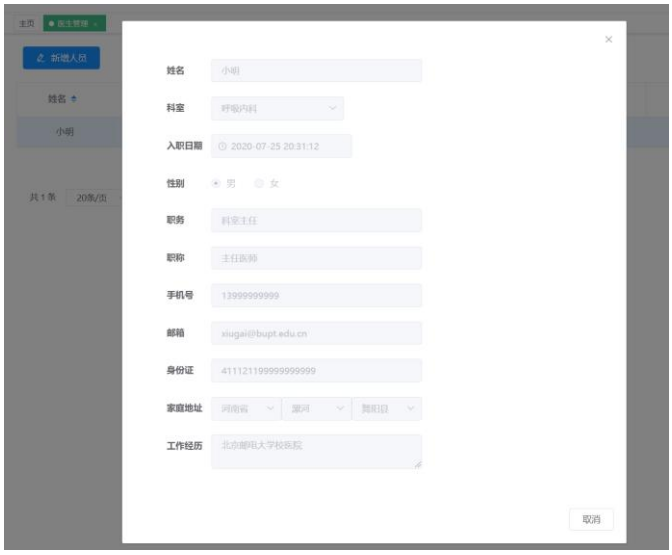
点击确认后，后端区块链将显示新增的区块，如下图所示。

接下来演示编辑操作，假设我们需要修改“小明”的邮箱，那么点击列表中小明对应的编辑按钮，即可打开编辑窗口，修改完成后点击确认按钮即可，如下图所示。



此时后端再次打印了区块链的内容，可以看到小明的邮箱已经修改了，而且区块的哈希值没有改变，如图 14 所示。

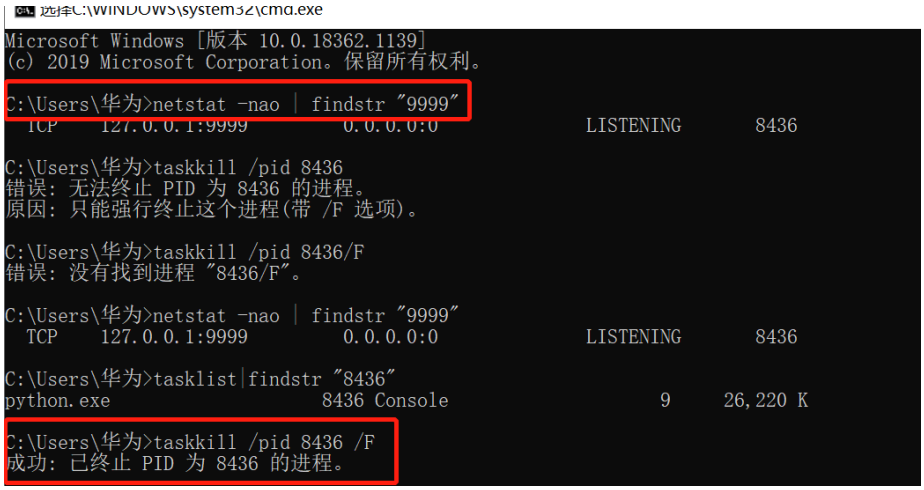
接下来，我们点击列表中小明对应的查看按钮，即可看到小明的个人信息，如下图所示，可以看到小明的邮箱是修改后的，且在查看窗口是无法编辑信息的。



注意：有事 python 端报错端口被占用，可以在 cmd 关闭占用端口的程序，端口为 9999，查询和关闭命令为：

netstat -nao | findstr "9999"

taskkill /pid 8436 /F


选择C:\WINDOWS\system32\cmd.exe
Microsoft Windows [版本 10.0.18362.1139]
(c) 2019 Microsoft Corporation。保留所有权利。
C:\Users\华为>netstat -nao | findstr "9999"
TCP 127.0.0.1:9999 0.0.0.0:0 LISTENING 8436
C:\Users\华为>taskkill /pid 8436
错误: 无法终止 PID 为 8436 的进程。
原因: 只能强行终止这个进程(带 /F 选项)。
C:\Users\华为>taskkill /pid 8436/F
错误: 没有找到进程 "8436/F"。
C:\Users\华为>netstat -nao | findstr "9999"
TCP 127.0.0.1:9999 0.0.0.0:0 LISTENING 8436
C:\Users\华为>tasklist|findstr "8436"
python.exe 8436 Console 9 26,220 K
C:\Users\华为>taskkill /pid 8436 /F
成功: 已终止 PID 为 8436 的进程。