README

SHA256

sha256.cpp是SHA256算法，输入一段内容会输出这段内容的hash值，代码中限制了最大输入内容不超过10000字节，但算法实际上是可以输入无限长字符的

```
please input the plain text:hello
2cf24dba
5fb0a30e
26e83b2a
c5b9e29e
1b161e5c
1fa7425e
73043362
938b9824
```

实验一

chain.cpp是实验说明SHA256如何用于区块数据锁定，不打开140行的注释前是修改前的模拟区块链内容，打开注释后是对某一块内容进行微小修改后区块链的内容，通过对比可以发现SHA256对微小改动做出的反应。实验模拟了短短5个区块形成的区块链修改前后的内容，第0个区块没有前节点所以没有hash值进行存放。

```
140         //chain[1][36]='2';little change
```

对数据做出修改之前的区块链内容如下：

```
chain[1]:facd9135830244f5f8a23029a2a243c0263a8d6c04db084ec92030f89908fc666461746132
chain[2]:972c78c472cbe19596080b2d1091f585ae9c209ec264cc5fe9389b55147ce3d86461746132
chain[3]:d2b8591fe7ebed21bf8137cdb2eb2c32457925e48a506f45134db51b9101e3976461746133
chain[4]:6060900e41cd2d64a77c0939456a2df88182285be78c5c5272b180bbafed198d6461746134

--------------------------------
```

修改之后的区块链内容出现了巨大的变化：

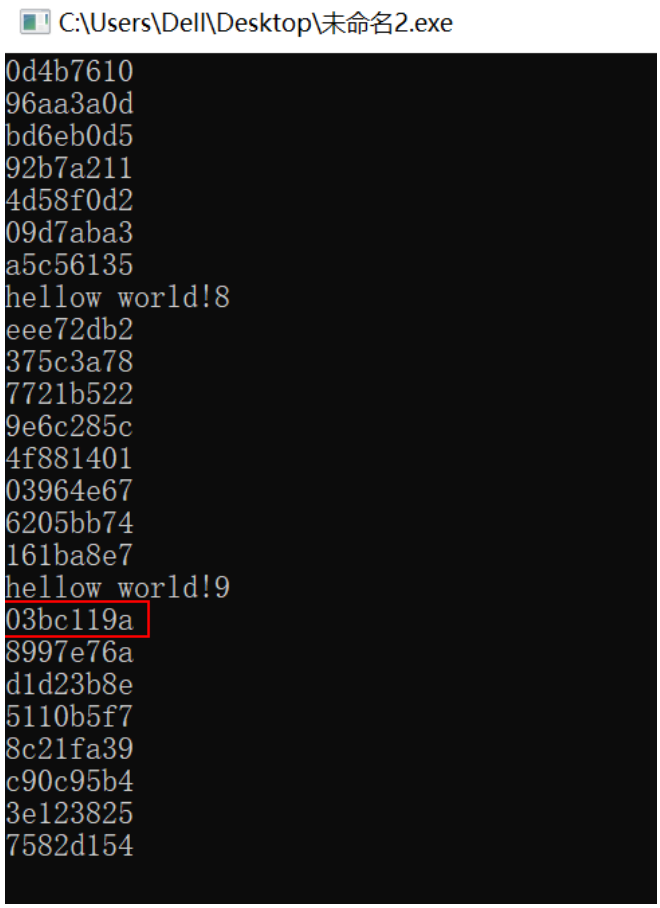
```
chain[1]:facd9135830244f5f8a23029a2a243c0263a8d6c04db084ec92030f89908fc666461746131
chain[2]:a5d7ac6d0edf1e21d84469a77368f9855b2f3c39d8e252dae4bc44428c1010a16461746132
chain[3]:9243dc5c9118b0c314dafd14b5d2eed3bc129ba580e0201bb35620ef3cb8212b6461746133
chain[4]:f88ffde31ff980e8f40073a596699603f00bd6a8f9d7976e266ab107dedd1c896461746134

--------------------------------
```

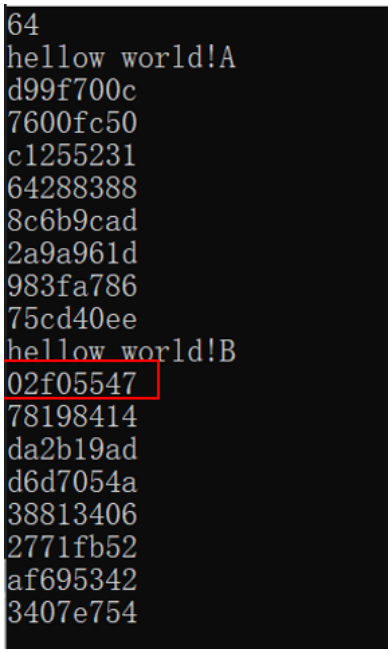
实验二

pow.cpp是实验模拟PoW工作过程，通过修改122行的条件可以控制前置共有多少位0，本实验由于电脑性能原因设置为前6位0，可以在较快时间得到结果

```
122     while((h[0]>>26)!=0){
```

实验几次结果，均能在较快时间内找到前6位为0的结果，改为8位后仅仅通过一轮循环已经无法得到结果





以上三个文件的.exe文件可以直接运行，实验的详细内容已上交邮箱