区块链实验报告

1. 存储设计

   用结构体实现存储，设计 block，transaction，input，output 四个结构体，数据元素类型按照题目要求。出于简洁考虑，Block 中的 transaction，transaction 中的 input 和 output 都用 vector 存储。此外，为方便之后的判断，在 transaction 中增加“int illegal”项，用来记录交易是否违法，在 output 中加入“int used”项，用来记录该 input 是否已经被使用。

   Block 按照单链表方式来进行存储。

2. 数据读入

   设计四个函数顺序分别读入 block，transaction，input 和 output，存入对应位置。

3. 非法交易判断

   对于每个交易:

   初始化 inputValue=0，遍历各个 input，用函数 countInput（）来计算 input 的总 value 值。

   countInput（）的返回值为所有 input 对应 output 的 value，同时根据不同的非法情况返回特定值如 0，-1，-2 来标记引用 transaction 非法，引用 output 已经被使用，引用 output 无法找到等情况。并对其进行特判，如果判断为非法情况，将目前交易的 illegal 赋值为 1，输出非法字串和非法原因。

   遍历 output，得到总的 outputValue。

   比较 inputValue 和 ouputValue 的大小，如果 inputValue 大于 outputValue，仍然为非法，illegal 赋值为 1，输出非法 id 和非法原因。

此部分源码:

```
int illegal(block *blocks)
{
    int count=0;
    block *head=blocks;
    while(blocks!=NULL)
    {
        for(auto &transactions :blocks->transactions)
        {
            long long inputValue=0;
            long long outputValue=0;
            if(transactions.is_coinbase)continue;
            inputValue=countInput(transactions,head);
            if(inputValue==-1)//-1 代表引用的交易非法
            {
                transactions.legal=0;
                count++;
                cout<<"id of illegal transactions:
"<<transactions.txid<<endl;
                cout<<"Height:"<<blocks->Height<<endl;
                cout<<"reanson is using an illegal output"<<endl;
                continue;
```

```
            }
            else if(inputValue==-2)//代表 input 已经被使用。
            {
                transactions.legal=0;
                count++;
                cout<<"id of illegal transactions:
"<<transactions.txid<<endl;
                cout<<"Height:"<<blocks->Height<<endl;
                cout<<"reason is using a used input"<<endl;
                continue;
            }
            else if(inputValue==0)//代表找不到交易
            {
                transactions.legal=0;
                count++;
                cout<<"id of illegal transactions:
"<<transactions.txid<<endl;
                cout<<"Height:"<<blocks->Height<<endl;
                cout<<"reason is can't find the input"<<endl;
            }
            else{
            for(auto output:transactions.outputs)
            {
                outputValue+=output.value;
            }
            if(outputValue>inputValue)
            {
                count++;
                cout<<"id of illegal transactions:
"<<transactions.txid<<endl;
                cout<<"Height:"<<blocks->Height<<endl;
                cout<<"reanson is input value less than output
value"<<endl;
                cout<<"(output value: "<<outputValue<<">input value:
"<<inputValue<<")"<<endl;
                transactions.legal=0;
            }
        }}
        blocks=blocks->nextblock;
    }
    return count;
}

long long countInput(transaction transactions,block *hd)
```

```
{
    int value=0;
    for(auto &in: transactions.inputs)
    {   int heigt=in.pre_block;
        block *blocks=hd;
        string id=in.prevTxID;
        while(blocks->Height!=heigt&&(blocks->nextblock!=NULL)){//找到
preHeight 对应区块
            blocks=blocks->nextblock;
        }
        int flag=0;
        for(auto &tr :blocks->transactions)//遍历区块的交易，找到所需要的。
        {
            if(tr.txid==id)
            {flag=1;
                if(tr.legal)
                {
                    if(!tr.outputs[in.prevTxOutIndex].used){
                    if(in.prevTxOutIndex<tr.output_count)
                    {value+=tr.outputs[in.prevTxOutIndex].value;
                    }
                    tr.outputs[in.prevTxOutIndex].used=1;}
                    else if(in.prevTxOutIndex>=tr.output_count){
                        return 0;
                    }
                    else{
                        return -2;
                    }
                }
                else{
                    return -1;
                }
            }
        }
        if(flag==0)
        {
            return 0;
        }
    }
    return value;
}
```

4. 交互界面设计

首先读入数据输出基本信息:

总区块数，总交易数，非法交易 ID 和原因，非法交易数，合法交易数和用户输入提示。

用户可输入 1，2，3 分别代表输入高度，ID 和退出。

如输入 1，之后再输入高度，可输出 block 中所有交易信息。

如输入 2，之后再输入 ID，可得到特定 id 的交易信息，同时如果找不到会提示未找到。

如输入 3，结束程序。

输入其他数字，提示操作非法，重新输入。

5. 输出截图

显示基本信息：

```
!!!Block!!!
Counts of blocks: 32490
Counts of transactions: 32709
id of illegal transactions: b76d8d9fe2082040018456b13825cd835cc703f870528b45cf0d36dc6a268961
Height:25552
reason is can't find the input
id of illegal transactions: 7bfa5a4a5d0ba60497f4c61b9ab3b289017cf5f9f9eb68c558614388f0383be6
Height:29430
reason is can't find the input
id of illegal transactions: 3a5769fb2126d870aded5fcaced3bc49fa9768436101895931adb5246e41e957
Height:29664
reanson is input value less than output value
(output value: 159544000>input value: 159543500)
id of illegal transactions: ec7ec389613dd485cf8786021afd547536f18c4aa131c50954d4df2353bb6f97
Height:29668
reanson is using an illegal output
id of illegal transactions: 66416b1cf7130aaff13e8a60bf0d0f7e66375bf7978ae032790102bf227ef7b9
Height:29775
reanson is using an illegal output
id of illegal transactions: 9843d685c90a2053dc80600ffd03f076da831502eec65cb3a152d7ee57a6120d
Height:31753
reason is can't find the input
Counts of illegal: 6
Counts of legal:32703
```

功能 1，输出高度对应信息：

```
Please enter next option(1:input height,2:input txID,3:quit):
1
Please input height:
5000
 Height:5000
 hash: 000000004d78d2a8a93a1d20a24d721268690bebd2b51f7e80657d57e226eef9
 prevHash: 00000000c9a61ea18fbf06b03e10033355e6eab3de038d975f40af9babbe0658
 transactions` txID:
  b0e585927e1737d07bd8157a2ba9f7615ef8ecd2af6d03523e51b4d23e134b6a
 ||is coinbase||
 output:
  index:0   value:500000
Please enter next option(1:input height,2:input txID,3:quit):
5000000
Illegal option,try again
Please enter next option(1:input height,2:input txID,3:quit):
1
Please input height:
5000000
No such Height!
Please enter next option(1:input height,2:input txID,3:quit):
```

功能 2，输出 ID 对应交易：

```
Please enter next option(1:input height,2:input txID,3:quit):
2
Please input ID:
7379f506dfccc392195aa5e2aea2b0d8a25f846023591c32d0c9e1fcfb7a0fff
 ||is coinbase||
 output:
  index:0   value:500000
Please enter next option(1:input height,2:input txID,3:quit):
2
Please input ID:
1231fasfsdfsfwf23r23fsdfwr2frgeg43g34gege
no such transaction!
Please enter next option(1:input height,2:input txID,3:quit):
```