## **实验02、区块的链**

1.背景

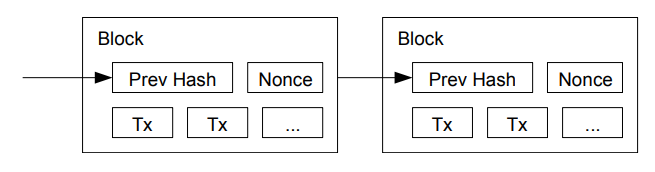


图1：区块示意图

区块链，就是一组区块构成的“链”，也就是链表。 下面关于区块和交易的定义来自比特币系统，根据任务需要作了简化。

在比特币系统中，采用的是UTXO模型，即每个交易将使用前面某个交易的输出(output)来作为当前交易的输入(input)。而当前交易的输出将作为未来某个交易的输入。

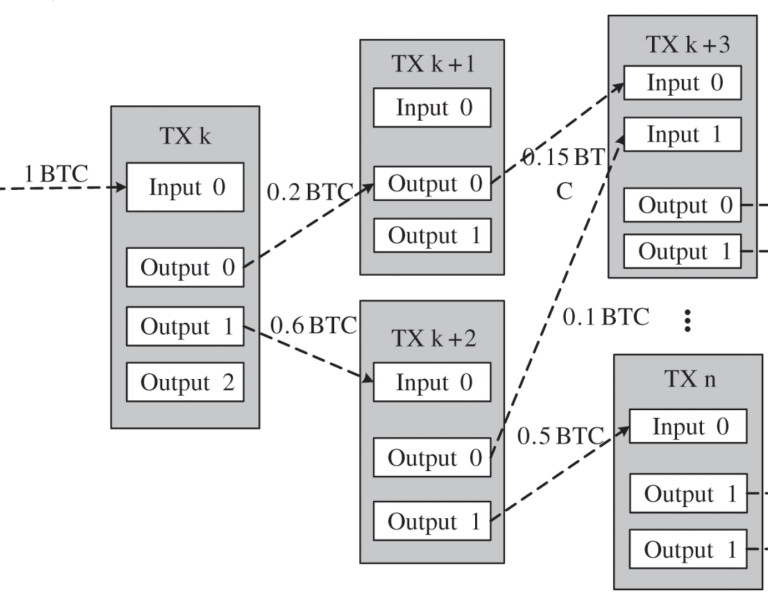


图2：UTXO模型

在本次实验中，我们需要定义如下结构体：

(1)区块(block)

其中包含了如下成员：

|  |  |  |
| --- | --- | --- |
| 成员名 | 类型 | 说明 |
| height | 整数 | 当前块的高度，一条链上每个区块的Height均不相同。 |
| hash | 字符串 | 本区块的哈希值。 |
| prevHash | 字符串 | 前一个区块的哈希值，本实验中可以置空 |
| merkleRoot | 字符串 | 本区块中所有交易的默克尔树根，本实验中可以置空 |
| nonce | 整数 | 神秘数，本实验可以忽略 |
| transactions | 数组 | 一组交易(transaction)的集合 |

1. 交易(transaction)

其中包含了如下成员：

|  |  |  |
| --- | --- | --- |
| 成员名 | 类型 | 说明 |
| txid | 字符串 | 交易的编号，具有唯一性 |
| input\_count | 整数 | inputs的数量，本实验可以忽略 |
| output\_count | 整数 | outpus的数量，本实验可以忽略 |
| inputs | 数组 | 一组input的集合，表示当前交易的输入所用到的输出 |
| outputs | 数组 | 一组output的集合，表示当前交易的输出，可能作为后续交易的输入 |
| is\_coinbase | 整数 | 表示是否为coinbase交易（1为coinbase交易，0为非coinbase交易，coinbase交易在下文解释） |

1. 输入(input)

其中包含了如下成员：

|  |  |  |
| --- | --- | --- |
| 成员名 | 类型 | 说明 |
| pre\_block | 整数 | 该input所引用的output所在区块的高度； |
| prevTxID | 字符串 | 该input所引用的output所在交易的txID |
| prevTxOutIndex | 整数 | 该input所引用的output位于所在交易output集合中的索引 |
| scriptSig | 字符串 | 脚本和签名，本实验中可以置空 |

1. 输出(output)

其中包含了如下成员：

|  |  |  |
| --- | --- | --- |
| 成员名 | 类型 | 说明 |
| txid | 字符串 | 该output所属的交易 |
| index | 整数 | 该output在所属交易中的索引值 |
| value | 整数 | 该output的价值(数据已乘10^8,避免浮点误差)，请用long long数据类型（int会溢出） |
| script | 字符串 | 脚本，本实验可以置空 |

2．目的

* 练习顺序表和链表的基本操作。
* 实现简单的区块和交易，为后续实验做准备。

1. 问题描述

* 读入区块相关数据文件(包括blocks.csv,transaction.csv,inputs.csv,outputs.csv四个，具体格式见输入实例)，生成区块数据变量，将多个区块存储在一个链表里面。
* 输入一个区块，检验其中交易的合法性：

一个交易可以有多个input，多个output。每个input会使用之前某个交易的output。规则如下：

a、每个input所使用的output 能够找到。

b、每个input所使用的output没有被之前的交易用过。

c、该交易所有input所引用的output 价值（value）之和 大于等于该交易所有output的价值（value）之和。

注意：

a、有一类特殊的交易，其is\_coinbase字段为true，该类交易的特点是没有input，只有output，但区块的input-count不为0，该类交易是合法的，其中的output可能被后续的transaction所引用。

b、每一个output只能被使用一次，即便还有剩余的value没有被使用

c、如果某个交易是非法的，那么引用了该交易作为input的交易也同样是非法的（非法交易不会被包括在区块内，如果使用了则相当于违反了规则a）

以如下输入作为示例（示例中在结构体说明里面可以置空的字段不再列出）：

block:

|  |  |  |
| --- | --- | --- |
| height | hash | prevHash |
| 0 | 0000000000000000000b88309 | 0000000000000000000a4fc08 |
| 1 | 0000000000000000000bb6561 | 0000000000000000000b88309 |
| 2 | 000000000000000000078848a | 0000000000000000000bb6561 |
| 3 | 00000000000000000002101d9 | 000000000000000000078848a |

transaction:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| height | txid | is\_coinbase | in-counter | out-counter |
| 0 | bb171757a76cd2c95 | 1 | 0 | 1 |
| 1 | bdf2c8a2482cc9ca5 | 0 | 1 | 2 |
| 2 | c5c36a7e0a7d7a95a | 0 | 1 | 2 |
| 3 | 5a916d9e74946ed6f | 0 | 1 | 2 |
| 3 | 1adacd29c4fddcfac | 0 | 1 | 2 |

inputs:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| height | txid | prev\_block | prevTxID | prevTxOutIndex |
| 1 | bdf2c8a2482cc9ca5 | 0 | bb171757a76cd2c95 | 0 |
| 2 | c5c36a7e0a7d7a95a | 1 | bdf2c8a2482cc9ca5 | 0 |
| 3 | 5a916d9e74946ed6f | 1 | bdf2c8a2482cc9ca5 | 0 |
| 3 | 1adacd29c4fddcfac | 2 | c5c36a7e0a7d7a95a | 0 |

outputs:

|  |  |  |  |
| --- | --- | --- | --- |
| height | txid | index | value |
| 0 | bb171757a76cd2c95 | 0 | 100000000 |
| 1 | bdf2c8a2482cc9ca5 | 0 | 28638715 |
| 1 | bdf2c8a2482cc9ca5 | 1 | 1637692 |
| 2 | c5c36a7e0a7d7a95a | 0 | 17366721 |
| 2 | c5c36a7e0a7d7a95a | 1 | 11221994 |
| 3 | 5a916d9e74946ed6f | 0 | 17366721 |
| 3 | 5a916d9e74946ed6f | 1 | 11221994 |
| 3 | 1adacd29c4fddcfac | 0 | 173667 |
| 3 | 1adacd29c4fddcfac | 1 | 21 |

从示例中可以看出：

1. 每个block中的prevHash为上一个block的hash，即“链”。
2. 区块0中的bb171757a76cd2c95交易为coinbase交易，其没有输入，只有1个输出，value 为100000000，是合法的。
3. 区块1中的bdf2c8a2482cc9ca5交易用了区块0中bb171757a76cd2c95交易的第0个输出作为输入，并且产生了两个输出。
4. 区块2中的c5c36a7e0a7d7a95a交易用了区块1中bdf2c8a2482cc9ca5交易的第0个输出作为输入，产生了两个输出，且两个输出的value之和(17366721+11221994=28588715)小于bdf2c8a2482cc9ca5交易的第0个输出的value(28638715),即交易合法。注意：尽管bdf2c8a2482cc9ca5交易的第0个输出的value没有被完全用完（28638715>28588715)，这个output也不能被再次使用
5. 区块3中的5a916d9e74946ed6f交易尝试使用bdf2c8a2482cc9ca5中的第0个输出作为输入，但这个输出在c5c36a7e0a7d7a95a中已经被使用，故该交易以及后续使用该交易作为输出的交易都视为非法
6. 区块3中的1adacd29c4fddcfac交易也是合法的
7. 具体要求

* 区块中的交易(transaction)集合，以及交易中的input和output，**均采用顺序表实现**。
* 采用双向循环链表实现（选做）。

1. 展示内容

* 能将所有区块按高度顺序组织成链表，打印链表长度。
* 输出以下统计信息：区块总数、合法交易总数、不合法的交易总数。
* 从键盘输入区块高度，输出该区块内容。
* 从键盘输入交易txID，输出该交易内容。

**在完成3个区块的小文件基础上，可以继续完成下面的内容：**

1. 进阶要求

* 下载2009data.zip，处理2009年比特币全部区块数据（CSV格式），找出里面的非法交易。
* 注意，比特币系统在2009年还处于萌芽期，绝大部分区块中只有一个交易，称为coinbase交易。