POW协议仿真 课程设计

518021910740 池彦廷

1.设计要求

实现一个PoW的多线程仿真程序，每个线程模拟一个节点生成区块链的状态
不需要完整构造Bitcoin的数据结构，有Hash、算力证明（计算也可通过随机数实现，1s左右出块）
可设置节点数量，测量区块链的增长速度
设置一定数量的恶意节点实施分叉攻击，即不在最长链构造区块
测量不同恶意节点比例（10%-40%）条件下，统计分叉攻击成功的次数

2.总体设计

2.1 区块设计

区块结构如下(block.go),各部分含义参照注释

```
type Block struct {
    // hash of the previous block
    Previous string
    // solution: like bitcoin
    Nonce uint64
    //  difficulty : how many zeros required
    Bits uint64
    // timestamp
    Timestamp int64

    Blockhash string
    /*-------------data part---------------*/
    // using a transformation of Bits and Previous as data
    Data string
    //  using in judge which chain is longer
    Height int64
}
```

其中BlockHash为区块的标识，Previous为上一个区块的BlockHash。Blockhash由BlockHead（Previous，Timestamp，Bits和Nonce）计算得来。

```
type BlockHead struct {
    Previous string `json:"prev"`
    Time     int64  `json:"time"`
    Bits     uint64 `json:"bits"`
    Nonce    uint64 `json:"nonce"`
}
```

Height记录当前区块在链中的高度，链中最大的Height即为区块链最长链的长度。
POW为类似比特币的方式实现，比特币区块中的交易信息由随机数Data模拟，Data和Nonce构成了区块中的数据部分。计算数据部分的merkleHash与sha256Hash得值V，若V的前Bits位为0则认为区块是满足工作量条件的。

2.2 矿工节点设计与挖矿流程

矿工节点node(node.go)设计如下，

```
type Node struct {
    // the identifier of node
    id          uint64
    // the message channel to broadcast block
    peers       map[uint64]chan Message
    // channel for each node
    receiveChan chan Message
    // chain buffer
    Buffer      map[string]block.Block
    // receive message (like stop and change bits) info from admin
    adminChan   chan AdminMessage
    // current difficulty
    Bits        uint64
}
```

其中buffer中存储着每个节点"认为"的区块链。adminChan为管理员节点发送信息AdminMessage所用的channel(如停止挖矿，改变Bits).

```
type AdminMessage struct {
    sender  uint64
    ifStop  bool
    newBits uint64
}
```

receiveChan接受Message信息，Message信息中包括发送者，新的区块以及是否为恶意节点的信息。为模拟需要，良性节点将会忽略恶意节点发送的Block。我们定义**良性Message**为isMal为false的Message,**恶性Message**则相反.

```
type Message struct {
    sender   uint64
    newBlock block.Block
    isMal    bool
}
```

矿工挖矿流程为：挖矿节点N不断产生区块，变换区块的Nonce直到产生符合POW阈值要求的区块B，N将B放入自己的Buffer中，并将这个区块通过peers通道广播给所有节点。

当另一个节点M收到区块后，将该区块放入自己的Buffer中，并计算新区块的高度。若高度大于自己目前正在挖的区块，则更改正在挖的区块，在B的基础上继续进行挖矿。

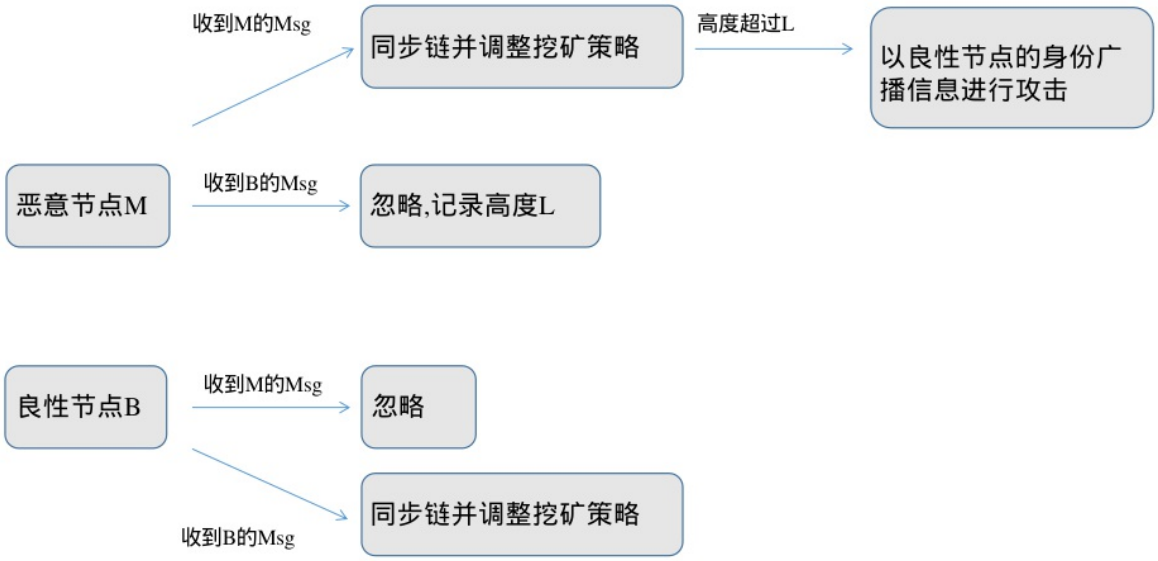
管理员节点(类似与比特币的Bits控制者)与普通节点一致并参与挖矿. 不同的是,管理员节点负责监控区块的增加速度并实时调控Bits,同时管理员节点可以发动信息令节点停止挖矿.

2.3 恶意节点与攻击设计

恶意节点的Node与发送的信息等结构体与普通节点相同，但是在挖矿成功后他们发送的Message中的isMal 为true。

当良性节点接收到恶意节点发送的消息M（通过isMal判断），它们会**忽略**这个消息并继续挖矿。
当恶意节点收到良性节点发送的消息M'时，它们会**记录M'中Block的Height属性**L（即良性区块链的最长链长度）并**丢弃**这一信息。

当恶意节点收到M时，它会正常处理该信息并将M中Block信息加入自己的Buffer中。即所有恶意节点与良性节点分开进行挖矿.若恶意节点的中Buffer最长块的高度高于良性节点中Buffer的高度,则恶意节点以良性节点的身份广播整个Buffer进行攻击. 整体攻击设计如下图所示



3.具体设计与源码介绍

3.1 BLOCK区块设计 block.go

位于/Block 文件夹中.主要定义了区块以及区块有关的运算与使用方法.区块的定义在2.1中已介绍.以下介绍几个重要函数

3.1.1 区块初始化Init (line 44)

```
func (block *Block) Init(prev string, bits uint64) {
    block.Previous = prev
    block.Bits = bits
    // using random value to init nonce
    rand.Seed(time.Now().UnixNano())
    block.Nonce = uint64(rand.Intn(100000000))
    block.Timestamp = time.Now().UnixNano()
    block.Data = fmt.Sprintf("%s%d", block.Previous, block.Bits)
    block.Blockhash = block.BlockHashCal()
    block.Height = NO_HEIGHT
}
```

用随机数初始化Nonce以加快不同节点的挖矿(使得不同节点开始的Nonce不同,减少重复运算).在检测可行性之前先计算Block的唯一标识BlockHash(Line 56,Blockhash由BlockHead（Previous，Timestamp，Bits和Nonce）计算得来。),并用常数-1初始化高度.

3.2.2 区块正确性检查 IsValid

```
func (block *Block) IsValid() bool {
    // for test only
    if block.Blockhash != block.BlockHashCal() {
        fmt.Printf("ERROR: Bad Block height %d, hash %s\n", block.Height,
block.Blockhash)
        return false
    }
    data := fmt.Sprintf("%s%d", block.Data, block.Nonce)
    dataHash := CalculateHash([]byte(data))

    for i := uint64(0); i <= block.Bits; i++ {
        if string(dataHash[i]) != "0" {
            return false
        }
    }
    // fmt.Println(dataHash)
    return true
}
```

IsValid检测区块是否满足工作量条件,类似比特币的计算方式但是**交易数据用随机数**进行模拟.如果计算的hash值的前Bits位均为0则满足POW条件,可以广播该区快.

3.3.3 区块高度计算 GetBlockHeight

用递归的方式计算区块高度,即每一个区块为Previous对应区块的Height+1,求Previous区块的高度时又会找Previous的Previous区块.这种方式计算量偏大,但是保证了任何时候区块链中的某一条链(往往是最长链)不会被篡改(若被篡改则递归计算高度时会发生错误)

```
func (block Block) GetBlockHeight(chain map[string]Block) int64 {
    // fmt.Printf("INFO: getting height of Block %s\n", block.Blockhash)
    if block.Previous == "FIRST" {
        return 0
    }
    if block.Height >= 0 {
        return block.Height
    }

    // find Previous Block in the map
    previousBlock, ifFind := chain[block.Previous]
    //debugging
    if !ifFind {
        if block.Previous == "FIRST" {
            // fmt.Println("INFO:in")
            return 0
        }
        fmt.Printf("ERROR: BLOCK %.5s NO prev block\n", block.Blockhash)
        // fmt.Println("warning！ no previous block find")
        return NO_HEIGHT
    } else {
        preHeight := previousBlock.GetBlockHeight(chain)
        if preHeight <= -1 {
            return NO_HEIGHT
        }
        // fmt.Println("INFO: prevHeight=", previousBlock.Height)
        block.Height = previousBlock.Height + 1
        // fmt.Println("INFO: height=", block.Height)
        chain[block.Blockhash] = block
        return chain[block.Blockhash].Height
    }

}
```

类似的,**GetLastBlock**遍历所有Block并找到高度最高的一个(即链中的最后一个区块).

3.2 矿工节点以及挖矿操作 miner.go

Miner/miner.go为主要程序部分,其定义了节点并调用block.go中的区块定义与操作进行挖矿.其中节点的定义与挖矿的简单流程,恶意节点的攻击流程见2.3,以下介绍重要函数

3.2.1 挖矿函数 Run MalRun

我们在挖矿函数中测量了**区块链的增长速度**
良性节点的挖矿函数Run函数位于miner.go的Line 72,伪代码与说明如下所示,详细代码见源码部分,说明见2.2

```
func (n *Node) Run() {

    定义调试信息,每10s准时输出链的长度信息
    ticker := time.NewTicker(time.Second * DEBUG_TIME)
    defer ticker.Stop()


    prevChainHeight := 0
    currentChainHeight := 0

    初始化,找到链中最高的节点,在该节点基础上进行挖矿
    fmt.Println("Node start : number ", n.id)
    startBlock := block.GetLastBlock(n.Buffer)
    信号接受与处理部分
    for {
        select {

        case msg := <-n.receiveChan: 接受到区块信息
            若为良性Msg则将Msg中的Block添加到Buffer中
            若为恶性则忽略

        case adminMsg := <-n.adminChan: 接受到管理员信息
            检查是否停止挖矿与改变Bits
        case <-ticker.C:接受到调试信息
            输出当前Buffer中的区块情况以及高度
        default:
            进行挖矿,调用Mine函数进行挖矿
            startBlock = n.Mine(startBlock)
        }
    }
}
```

恶意节点的挖矿函数MalRun位于Line 165,其功能大致与Mine相同,在**接受msg区块消息的部分**以及**挖矿函数**部分有差别

```
func (n *Node) MalRun() {
    定义调试信息,每10s准时输出链的长度信息
    ticker := time.NewTicker(time.Second * DEBUG_TIME)
    defer ticker.Stop()


    originalHeight := startBlock.Height
    benignHeight用于记录良性节点的高度
    检查攻击是否成功
    benignHeight := int64(block.NO_HEIGHT)
    信号接受与处理部分
    for {
        select {
        case msg := <-n.receiveChan:
            如果接受到恶意Msg,则将Block存至Buffer中并改变挖矿的起始区块
            如果收到良性Msg则记录当前良性节点的最高高度
        case adminMsg := <-n.adminChan:
            检查是否停止挖矿与改变Bits
        case <-ticker.C:
            输出当前Buffer中的区块情况以及高度,测试区块链增长速度
        default:
            用MalMine函数进行挖矿
            startBlock = n.MalMine(startBlock, benignHeight, originalHeight)
        }
    }
}
```

3.2.2 挖矿函数 Mine Malmine

Mine函数位于Line 147,被Run所调用. 其功能为不断产生新的区块并检测它们是否满足工作量条件,若满足则广播该区快.

```
func (n *Node) Mine(startBlock block.Block) block.Block {
    newBlock := block.Block{}
    newBlock.Init(startBlock.Blockhash, n.Bits)
    if newBlock.IsValid() {
        n.Buffer[newBlock.Blockhash] = newBlock
        newBlock.Height = newBlock.GetBlockHeight(n.Buffer)
        //broadcast msg to node
        msg := Message{sender: n.id, newBlock: newBlock, isMal: false}
        n.Broadcast(msg)
        return newBlock
    } else {
        // fmt.Printf("INFO: node %d has calculated a wrong block with nonce %d
\n", n.id, newBlock.Nonce)
        return startBlock
    }
}
```

MalMine函数位于Line 231. 其功能在Mine的基础上判断是否攻击成功(即恶意节点构造的区块高度高过了良性节点构造的区块高度).若攻击成功则发送自己的恶意链作为**良性信息**给良性节点进行攻击.

```
func (n *Node) MalMine(startBlock block.Block, benignHeight int64, originHeight
int64) block.Block {
    newBlock := block.Block{}
    newBlock.Init(startBlock.Blockhash, n.Bits)
    if newBlock.IsValid() {
        n.Buffer[newBlock.Blockhash] = newBlock
        newBlock.Height = newBlock.GetBlockHeight(n.Buffer)
        //broadcast msg to Malnode
        fmt.Printf("INFO: Malnode %d has generated new block with hash %.5s\n",
n.id, newBlock.Blockhash)
        msg := Message{sender: n.id, newBlock: newBlock, isMal: true}
        n.Broadcast(msg)
        //check if broadcast
        // if the benign chain has gone 2 blocks forward and the malchain goes
before the benign chain, we will broadcast
        if newBlock.Height > benignHeight && benignHeight > originHeight {
            fmt.Printf("INFO:ATTACK SUCCESS! current benign height: %d, mal
height %d\n", benignHeight, newBlock.Height)
            for _, block := range n.Buffer {
                if block.Height > originHeight {
                    msg := Message{sender: n.id, newBlock: block, isMal: false}
                    fmt.Printf("INFO: ATTACKER block sent\n")
                    n.Broadcast(msg)
                    os.Exit(0)
                }
            }
        }
        return newBlock

    } else {
        // fmt.Printf("INFO: node %d has calculated a wrong block with nonce %d
\n", n.id, newBlock.Nonce)
        return startBlock
    }
}
```

3.2.3 广播函数 BroadCast与AdminBroadCast

广播函数位于Line263-Line290,主要用于将Msg与AdminMsg广播到各个节点.

3.2.4 管理员节点广播函数 StopAll与AdjustBits

位于Line 300,函数用于调整Bits以及关闭节点.

3.4 测试函数test.go

Test/test.go中定义了一个可控制恶意结点与良性节点数量的测试函数Test Line13. Test通过
定义了管理员节点以及数个普通节点,调用Mine以及Block中的函数利用多线程同步进行挖矿.

其中,**管理员节点**(在程序中为节点0)(类似与比特币的Bits控制者)与普通节点一致并参与挖矿. 不同的是,管理员节点负责监控区块的增加速度并实时调控Bits,同时管理员节点可以发动信息令节点停止挖矿.
在测试程序中,由于Bits从2逐渐变到4时,挖矿效率变化太多,便不测试变化Bits的内容.在挖矿过程中按下enter

就能成功停止所有节点

```
func Test(benNodeNum int, malNodeNum int) {
    //init create FirstBlock and chain
    totalNodeNum := benNodeNum + malNodeNum
    firstBlock := block.Block{Previous: "FIRST", Nonce: 0, Bits: 10, Timestamp:
time.Now().UnixNano(), Data: "This is the first!", Height: 0}
    firstBlock.Blockhash = firstBlock.BlockHashCal()
    chain := make(map[string]block.Block)
    chain[firstBlock.Blockhash] = firstBlock

    peers := make(map[uint64]chan node.Message)
    peers[0] = make(chan node.Message)

    adminPeers := make(map[uint64]chan node.AdminMessage)
    adminMsgChan := make(chan node.AdminMessage)
    adminPeers[0] = adminMsgChan
    adminNode := node.Node{}
    adminNode.Init(0, peers, adminMsgChan, chain, 3)

    // add Node

    nodeAdminChan := make([]chan node.AdminMessage, totalNodeNum-1)
    newNode := make([]node.Node, totalNodeNum-1)
    for i := 0; i < totalNodeNum-1; i++ {
        newNode[i] = node.Node{}
        newNode[i].Init(uint64(i+1), peers, nodeAdminChan[i], adminNode.Buffer,
adminNode.Bits)
        adminPeers[uint64(i)+1] = nodeAdminChan[i]
    }

    // newNode.Init(1, peers, nodeAdminChan, adminNode.Buffer, adminNode.Bits)

    fmt.Println("Init Complete")
    // peers test
    // for k, _ := range adminPeers {
    //  fmt.Println(k)
    // }
    var wg sync.WaitGroup
    wg.Add(totalNodeNum)
    // start all nodes
    go func(i0 int) {
        adminNode.Run()
        wg.Done()
    }(0)
    for j := 0; j < benNodeNum-1; j++ {
        go func(i0 int) {
            newNode[i0].Run()
            wg.Done()
        }(j)
    }
    if malNodeNum > 0 {
```

```
        for j := benNodeNum - 1; j < totalNodeNum-1; j++ {
            go func(i0 int) {
                newNode[i0].MalRun()
                wg.Done()
            }(j)
        }
    }
    for {
        n,_:=os.Stdin.Read(make([]byte, 5))
        if(n==1){
            fmt.Println("stop")
            adminNode.StopAll(adminPeers)
            break
        }
    }

    wg.Wait()
}
```

4.测试

用Test(9,1)测试运行结果如附录1中所示,可以看到,节点挖矿正常,最后输出得到的良性节点结果一致,恶性节点结果一致.
Test(3,3)并攻击成功的结果如5.2中所示,可以看到,在攻击成功后,所有良性节点抛弃了原有的结果而在恶意节点的链的基础上进行挖矿.

恶意节点为10%时,良性节点被成功进攻概率(恶意节点的区块链长过普通节点的区块链至少1块,且认为10s之后进攻仍不成功为进攻失败)概率为15%(3/20),恶意节点为30%时(6/20)进攻成功概率为30%. 均较为符合预期结果,且进攻时机为

5.附录

5.1 测试结果

```
Node Init: number 0
Node Init: number 1
Node Init: number 2
Node Init: number 3
Node Init: number 4
Node Init: number 5
Node Init: number 6
Node Init: number 7
Node Init: number 8
Node Init: number 9
Init Complete
MalNode start : number  9
Node start : number  0
Node start : number  4
Node start : number  2
Node start : number  7
Node start : number  3
```

```
Node start : number  6
Node start : number  8
Node start : number  5
Node start : number  1
INFO: node 1 has generated new block with hash 1f805
INFO: node 5 received INFO from 1
INFO: node 5 change the startBlock
INFO: node 7 received INFO from 1
INFO: node 7 change the startBlock
INFO: node 0 received INFO from 1
INFO: node 0 change the startBlock
INFO: node 2 received INFO from 1
INFO: node 2 change the startBlock
INFO: node 3 received INFO from 1
INFO: node 3 change the startBlock
INFO: node 4 received INFO from 1
INFO: node 4 change the startBlock
INFO: node 6 received INFO from 1
INFO: node 6 change the startBlock
INFO: node 8 received INFO from 1
INFO: node 8 change the startBlock
INFO: node 2 has generated new block with hash 15add
INFO: node 4 received INFO from 2
INFO: node 4 change the startBlock
INFO: node 6 received INFO from 2
INFO: node 6 change the startBlock
INFO: node 8 received INFO from 2
INFO: node 8 change the startBlock
INFO: node 5 received INFO from 2
INFO: node 5 change the startBlock
INFO: node 7 received INFO from 2
INFO: node 7 change the startBlock
INFO: node 0 received INFO from 2
INFO: node 0 change the startBlock
INFO: node 1 received INFO from 2
INFO: node 1 change the startBlock
INFO: node 3 received INFO from 2
INFO: node 3 change the startBlock
INFO: node 7 has generated new block with hash af79b
INFO: node 0 received INFO from 7
INFO: node 0 change the startBlock
INFO: node 1 received INFO from 7
INFO: node 1 change the startBlock
INFO: node 2 received INFO from 7
INFO: node 2 change the startBlock
INFO: node 3 received INFO from 7
INFO: node 3 change the startBlock
INFO: node 5 received INFO from 7
INFO: node 5 change the startBlock
INFO: node 4 received INFO from 7
INFO: node 4 change the startBlock
INFO: node 6 received INFO from 7
```

```
INFO: node 6 change the startBlock
INFO: node 8 received INFO from 7
INFO: node 8 change the startBlock
INFO: Malnode 9 has generated new block with hash 860d4
INFO: node 0 skipped malBlock
INFO: node 1 skipped malBlock
INFO: node 2 skipped malBlock
INFO: node 3 skipped malBlock
INFO: node 5 skipped malBlock
INFO: node 7 skipped malBlock
INFO: node 4 skipped malBlock
INFO: node 6 skipped malBlock
INFO: node 8 skipped malBlock
INFO: node 1 has generated new block with hash c49a3
INFO: node 4 received INFO from 1
INFO: node 4 change the startBlock
INFO: node 6 received INFO from 1
INFO: node 6 change the startBlock
INFO: node 8 received INFO from 1
INFO: node 8 change the startBlock
INFO: node 0 received INFO from 1
INFO: node 0 change the startBlock
INFO: node 2 received INFO from 1
INFO: node 2 change the startBlock
INFO: node 3 received INFO from 1
INFO: node 3 change the startBlock
INFO: node 5 received INFO from 1
INFO: node 5 change the startBlock
INFO: node 7 received INFO from 1
INFO: node 7 change the startBlock
INFO: Malnode 9 has generated new block with hash 74c0a
INFO: node 1 skipped malBlock
INFO: node 2 skipped malBlock
INFO: node 3 skipped malBlock
INFO: node 5 skipped malBlock
INFO: node 7 skipped malBlock
INFO: node 0 skipped malBlock
INFO: node 6 skipped malBlock
INFO: node 8 skipped malBlock
INFO: node 4 skipped malBlock
INFO: node 8 has generated new block with hash 09620
INFO: node 4 received INFO from 8
INFO: node 4 change the startBlock
INFO: node 6 received INFO from 8
INFO: node 6 change the startBlock
INFO: node 0 received INFO from 8
INFO: node 0 change the startBlock
INFO: node 1 received INFO from 8
INFO: node 1 change the startBlock
INFO: node 2 received INFO from 8
INFO: node 2 change the startBlock
INFO: node 3 received INFO from 8
```

```
INFO: node 3 change the startBlock
INFO: node 5 received INFO from 8
INFO: node 5 change the startBlock
INFO: node 7 received INFO from 8
INFO: node 7 change the startBlock
INFO: node 2 has generated new block with hash e75f8
INFO: node 6 received INFO from 2
INFO: node 6 change the startBlock
INFO: node 8 received INFO from 2
INFO: node 8 change the startBlock
INFO: node 4 received INFO from 2
INFO: node 4 change the startBlock
INFO: node 1 received INFO from 2
INFO: node 1 change the startBlock
INFO: node 3 received INFO from 2
INFO: node 3 change the startBlock
INFO: node 5 received INFO from 2
INFO: node 5 change the startBlock
INFO: node 7 received INFO from 2
INFO: node 7 change the startBlock
INFO: node 0 received INFO from 2
INFO: node 0 change the startBlock
INFO: Malnode 9 has generated new block with hash 2f040
INFO: node 6 skipped malBlock
INFO: node 8 skipped malBlock
INFO: node 4 skipped malBlock
INFO: node 1 skipped malBlock
INFO: node 2 skipped malBlock
INFO: node 3 skipped malBlock
INFO: node 5 skipped malBlock
INFO: node 7 skipped malBlock
INFO: node 0 skipped malBlock
INFO: node 3 has generated new block with hash 3a032
INFO: node 1 received INFO from 3
INFO: node 1 change the startBlock
INFO: node 2 received INFO from 3
INFO: node 2 change the startBlock
INFO: node 5 received INFO from 3
INFO: node 5 change the startBlock
INFO: node 7 received INFO from 3
INFO: node 7 change the startBlock
INFO: node 0 received INFO from 3
INFO: node 0 change the startBlock
INFO: node 6 received INFO from 3
INFO: node 6 change the startBlock
INFO: node 8 received INFO from 3
INFO: node 8 change the startBlock
INFO: node 4 received INFO from 3
INFO: node 4 change the startBlock
INFO: node 1 has generated new block with hash 6e916
INFO: node 4 received INFO from 1
INFO: node 4 change the startBlock
```

```
INFO: node 6 received INFO from 1
INFO: node 6 change the startBlock
INFO: node 8 received INFO from 1
INFO: node 8 change the startBlock
INFO: node 0 received INFO from 1
INFO: node 0 change the startBlock
INFO: node 2 received INFO from 1
INFO: node 2 change the startBlock
INFO: node 3 received INFO from 1
INFO: node 3 change the startBlock
INFO: node 5 received INFO from 1
INFO: node 5 change the startBlock
INFO: node 7 received INFO from 1
INFO: node 7 change the startBlock
INFO: node 3 has generated new block with hash 2e1e4
INFO: node 0 received INFO from 3
INFO: node 0 change the startBlock
INFO: node 1 received INFO from 3
INFO: node 1 change the startBlock
INFO: node 2 received INFO from 3
INFO: node 2 change the startBlock
INFO: node 5 received INFO from 3
INFO: node 5 change the startBlock
INFO: node 7 received INFO from 3
INFO: node 7 change the startBlock
INFO: node 4 received INFO from 3
INFO: node 4 change the startBlock
INFO: node 6 received INFO from 3
INFO: node 6 change the startBlock
INFO: node 8 received INFO from 3
INFO: node 8 change the startBlock
INFO: node 1 has generated new block with hash a9200
INFO: node 4 received INFO from 1
INFO: node 4 change the startBlock
INFO: node 6 received INFO from 1
INFO: node 6 change the startBlock
INFO: node 8 received INFO from 1
INFO: node 8 change the startBlock
INFO: node 5 received INFO from 1
INFO: node 5 change the startBlock
INFO: node 7 received INFO from 1
INFO: node 7 change the startBlock
INFO: node 0 received INFO from 1
INFO: node 0 change the startBlock
INFO: node 2 received INFO from 1
INFO: node 2 change the startBlock
INFO: node 3 received INFO from 1
INFO: node 3 change the startBlock
INFO: node 0 has generated new block with hash 3c149
INFO: node 2 received INFO from 0
INFO: node 2 change the startBlock
INFO: node 3 received INFO from 0
```

```
INFO: node 3 change the startBlock
INFO: node 5 received INFO from 0
INFO: node 5 change the startBlock
INFO: node 7 received INFO from 0
INFO: node 7 change the startBlock
INFO: node 1 received INFO from 0
INFO: node 1 change the startBlock
INFO: node 8 received INFO from 0
INFO: node 8 change the startBlock
INFO: node 4 received INFO from 0
INFO: node 4 change the startBlock
INFO: node 6 received INFO from 0
INFO: node 6 change the startBlock
INFO: node 6 has generated new block with hash 6bb1d
INFO: node 0 received INFO from 6
INFO: node 0 change the startBlock
INFO: node 1 received INFO from 6
INFO: node 1 change the startBlock
INFO: node 2 received INFO from 6
INFO: node 2 change the startBlock
INFO: node 3 received INFO from 6
INFO: node 3 change the startBlock
INFO: node 5 received INFO from 6
INFO: node 5 change the startBlock
INFO: node 7 received INFO from 6
INFO: node 7 change the startBlock
INFO: node 4 received INFO from 6
INFO: node 4 change the startBlock
INFO: node 8 received INFO from 6
INFO: node 8 change the startBlock
INFO: node 8 has generated new block with hash 5cd9c
INFO: node 4 received INFO from 8
INFO: node 4 change the startBlock
INFO: node 6 received INFO from 8
INFO: node 6 change the startBlock
INFO: node 0 received INFO from 8
INFO: node 0 change the startBlock
INFO: node 1 received INFO from 8
INFO: node 1 change the startBlock
INFO: node 2 received INFO from 8
INFO: node 2 change the startBlock
INFO: node 3 received INFO from 8
INFO: node 3 change the startBlock
INFO: node 5 received INFO from 8
INFO: node 5 change the startBlock
INFO: node 7 received INFO from 8
INFO: node 7 change the startBlock
INFO: node 7 has generated new block with hash 2f247
INFO: node 4 received INFO from 7
INFO: node 4 change the startBlock
INFO: node 6 received INFO from 7
INFO: node 6 change the startBlock
```

```
INFO: node 8 received INFO from 7
INFO: node 8 change the startBlock
INFO: node 3 received INFO from 7
INFO: node 3 change the startBlock
INFO: node 5 received INFO from 7
INFO: node 5 change the startBlock
INFO: node 0 received INFO from 7
INFO: node 0 change the startBlock
INFO: node 1 received INFO from 7
INFO: node 1 change the startBlock
INFO: node 2 received INFO from 7
INFO: node 2 change the startBlock
INFO: node 5 has generated new block with hash 980cd
INFO: node 7 received INFO from 5
INFO: node 7 change the startBlock
INFO: node 0 received INFO from 5
INFO: node 0 change the startBlock
INFO: node 1 received INFO from 5
INFO: node 1 change the startBlock
INFO: node 2 received INFO from 5
INFO: node 2 change the startBlock
INFO: node 3 received INFO from 5
INFO: node 3 change the startBlock
INFO: node 4 received INFO from 5
INFO: node 4 change the startBlock
INFO: node 6 received INFO from 5
INFO: node 6 change the startBlock
INFO: node 8 received INFO from 5
INFO: node 8 change the startBlock
INFO: Malnode 9 has generated new block with hash eef7f
INFO: node 8 skipped malBlock
INFO: node 4 skipped malBlock
INFO: node 6 skipped malBlock
INFO: node 2 skipped malBlock
INFO: node 3 skipped malBlock
INFO: node 5 skipped malBlock
INFO: node 7 skipped malBlock
INFO: node 0 skipped malBlock
INFO: node 1 skipped malBlock
INFO: node 0 has generated new block with hash 71145
INFO: node 8 received INFO from 0
INFO: node 8 change the startBlock
INFO: node 4 received INFO from 0
INFO: node 4 change the startBlock
INFO: node 6 received INFO from 0
INFO: node 6 change the startBlock
INFO: node 2 received INFO from 0
INFO: node 2 change the startBlock
INFO: node 3 received INFO from 0
INFO: node 3 change the startBlock
INFO: node 5 received INFO from 0
INFO: node 5 change the startBlock
```

```
INFO: node 7 received INFO from 0
INFO: node 7 change the startBlock
INFO: node 1 received INFO from 0
INFO: node 1 change the startBlock
INFO: node 0 has generated new block with hash b518f
INFO: node 1 received INFO from 0
INFO: node 1 change the startBlock
INFO: node 2 received INFO from 0
INFO: node 2 change the startBlock
INFO: node 3 received INFO from 0
INFO: node 3 change the startBlock
INFO: node 5 received INFO from 0
INFO: node 5 change the startBlock
INFO: node 7 received INFO from 0
INFO: node 7 change the startBlock
INFO: node 4 received INFO from 0
INFO: node 4 change the startBlock
INFO: node 6 received INFO from 0
INFO: node 6 change the startBlock
INFO: node 8 received INFO from 0
INFO: node 8 change the startBlock
INFO: current chain for node 1:
,height: 17BLOCK: prev 3a032, self 6e916, height 8
BLOCK: prev 2e1e4, self a9200, height 10
BLOCK: prev 5cd9c, self 2f247, height 14
BLOCK: prev 15add, self af79b, height 3
BLOCK: prev c49a3, self 09620, height 5
BLOCK: prev e75f8, self 3a032, height 7
BLOCK: prev 6bb1d, self 5cd9c, height 13
BLOCK: prev 2f247, self 980cd, height 15
BLOCK: prev 71145, self b518f, height 17
BLOCK: prev FIRST, self 2f5ba, height 0
BLOCK: prev 1f805, self 15add, height 2
BLOCK: prev 09620, self e75f8, height 6
BLOCK: prev a9200, self 3c149, height 11
BLOCK: prev 3c149, self 6bb1d, height 12
BLOCK: prev 2f5ba, self 1f805, height 1
BLOCK: prev af79b, self c49a3, height 4
BLOCK: prev 6e916, self 2e1e4, height 9
BLOCK: prev 980cd, self 71145, height 16
INFO: current chain for node 7:
,height: 17BLOCK: prev c49a3, self 09620, height 5
BLOCK: prev 09620, self e75f8, height 6
BLOCK: prev e75f8, self 3a032, height 7
BLOCK: prev 6e916, self 2e1e4, height 9
BLOCK: prev 980cd, self 71145, height 16
BLOCK: prev 71145, self b518f, height 17
BLOCK: prev FIRST, self 2f5ba, height 0
BLOCK: prev 3a032, self 6e916, height 8
BLOCK: prev 3c149, self 6bb1d, height 12
BLOCK: prev 2f5ba, self 1f805, height 1
BLOCK: prev 6bb1d, self 5cd9c, height 13
```

```
BLOCK: prev 5cd9c, self 2f247, height 14
BLOCK: prev 2f247, self 980cd, height 15
BLOCK: prev 1f805, self 15add, height 2
BLOCK: prev af79b, self c49a3, height 4
BLOCK: prev 2e1e4, self a9200, height 10
BLOCK: prev a9200, self 3c149, height 11
INFO: current chain for node 4:
,height: 17BLOCK: prev af79b, self c49a3, height 4
BLOCK: prev 09620, self e75f8, height 6
BLOCK: prev 3a032, self 6e916, height 8
BLOCK: prev 2f247, self 980cd, height 15
BLOCK: prev 2f5ba, self 1f805, height 1
BLOCK: prev 6e916, self 2e1e4, height 9
BLOCK: prev 3c149, self 6bb1d, height 12
BLOCK: prev 5cd9c, self 2f247, height 14
BLOCK: prev 980cd, self 71145, height 16
BLOCK: prev 1f805, self 15add, height 2
BLOCK: prev 15add, self af79b, height 3
BLOCK: prev e75f8, self 3a032, height 7
BLOCK: prev a9200, self 3c149, height 11
BLOCK: prev 71145, self b518f, height 17
BLOCK: prev FIRST, self 2f5ba, height 0
BLOCK: prev c49a3, self 09620, height 5
BLOCK: prev 2e1e4, self a9200, height 10
BLOCK: prev 6bb1d, self 5cd9c, height 13
GROWTH RATE INFO: 17 blocks generated during last 10 seconds
BLOCK: prev 15add, self af79b, height 3
INFO: current chain for node 0:
,height: 17BLOCK: prev FIRST, self 2f5ba, height 0
BLOCK: prev 1f805, self 15add, height 2
BLOCK: prev 09620, self e75f8, height 6
BLOCK: prev 2e1e4, self a9200, height 10
BLOCK: prev 3c149, self 6bb1d, height 12
BLOCK: prev 6bb1d, self 5cd9c, height 13
BLOCK: prev 5cd9c, self 2f247, height 14
BLOCK: prev 2f5ba, self 1f805, height 1
BLOCK: prev 15add, self af79b, height 3
BLOCK: prev 3a032, self 6e916, height 8
BLOCK: prev 6e916, self 2e1e4, height 9
BLOCK: prev a9200, self 3c149, height 11
BLOCK: prev 2f247, self 980cd, height 15
BLOCK: prev 980cd, self 71145, height 16
BLOCK: prev 71145, self b518f, height 17
BLOCK: prev af79b, self c49a3, height 4
BLOCK: prev c49a3, self 09620, height 5
BLOCK: prev e75f8, self 3a032, height 7
INFO: current chain for node 3:
,height: 17BLOCK: prev 15add, self af79b, height 3
BLOCK: prev e75f8, self 3a032, height 7
BLOCK: prev 2e1e4, self a9200, height 10
BLOCK: prev 6bb1d, self 5cd9c, height 13
BLOCK: prev 5cd9c, self 2f247, height 14
```

```
BLOCK: prev 71145, self b518f, height 17
BLOCK: prev FIRST, self 2f5ba, height 0
BLOCK: prev 1f805, self 15add, height 2
BLOCK: prev 980cd, self 71145, height 16
BLOCK: prev af79b, self c49a3, height 4
BLOCK: prev a9200, self 3c149, height 11
BLOCK: prev 3c149, self 6bb1d, height 12
BLOCK: prev 2f5ba, self 1f805, height 1
BLOCK: prev 6e916, self 2e1e4, height 9
BLOCK: prev 3a032, self 6e916, height 8
BLOCK: prev 2f247, self 980cd, height 15
BLOCK: prev c49a3, self 09620, height 5
BLOCK: prev 09620, self e75f8, height 6
INFO: current chain for node 2:
,height: 17BLOCK: prev 2e1e4, self a9200, height 10
BLOCK: prev a9200, self 3c149, height 11
BLOCK: prev 09620, self e75f8, height 6
BLOCK: prev 15add, self af79b, height 3
BLOCK: prev c49a3, self 09620, height 5
BLOCK: prev 6e916, self 2e1e4, height 9
BLOCK: prev 3c149, self 6bb1d, height 12
BLOCK: prev 5cd9c, self 2f247, height 14
BLOCK: prev 71145, self b518f, height 17
BLOCK: prev FIRST, self 2f5ba, height 0
BLOCK: prev 1f805, self 15add, height 2
BLOCK: prev 3a032, self 6e916, height 8
BLOCK: prev 2f247, self 980cd, height 15
BLOCK: prev 2f5ba, self 1f805, height 1
BLOCK: prev e75f8, self 3a032, height 7
BLOCK: prev 6bb1d, self 5cd9c, height 13
BLOCK: prev 980cd, self 71145, height 16
BLOCK: prev af79b, self c49a3, height 4
INFO: current chain for node 9:
,height: 4BLOCK: prev 860d4, self 74c0a, height 2
BLOCK: prev 74c0a, self 2f040, height 3
BLOCK: prev 2f040, self eef7f, height 4
BLOCK: prev FIRST, self 2f5ba, height 0
BLOCK: prev 2f5ba, self 860d4, height 1
INFO: MalNode 9 exited
INFO: current chain for node 8:
,height: 17BLOCK: prev 2f5ba, self 1f805, height 1
BLOCK: prev c49a3, self 09620, height 5
BLOCK: prev 3c149, self 6bb1d, height 12
BLOCK: prev 2e1e4, self a9200, height 10
BLOCK: prev 980cd, self 71145, height 16
BLOCK: prev 6bb1d, self 5cd9c, height 13
BLOCK: prev 71145, self b518f, height 17
BLOCK: prev 1f805, self 15add, height 2
BLOCK: prev 15add, self af79b, height 3
BLOCK: prev af79b, self c49a3, height 4
BLOCK: prev 3a032, self 6e916, height 8
BLOCK: prev 6e916, self 2e1e4, height 9
```

```
BLOCK: prev 2f247, self 980cd, height 15
BLOCK: prev FIRST, self 2f5ba, height 0
BLOCK: prev 09620, self e75f8, height 6
BLOCK: prev e75f8, self 3a032, height 7
BLOCK: prev a9200, self 3c149, height 11
BLOCK: prev 5cd9c, self 2f247, height 14
INFO: current chain for node 5:
,height: 17BLOCK: prev 1f805, self 15add, height 2
BLOCK: prev af79b, self c49a3, height 4
BLOCK: prev 2e1e4, self a9200, height 10
BLOCK: prev FIRST, self 2f5ba, height 0
BLOCK: prev 3c149, self 6bb1d, height 12
BLOCK: prev 5cd9c, self 2f247, height 14
BLOCK: prev a9200, self 3c149, height 11
BLOCK: prev 6bb1d, self 5cd9c, height 13
BLOCK: prev 980cd, self 71145, height 16
BLOCK: prev 71145, self b518f, height 17
BLOCK: prev 15add, self af79b, height 3
BLOCK: prev c49a3, self 09620, height 5
BLOCK: prev 3a032, self 6e916, height 8
BLOCK: prev 6e916, self 2e1e4, height 9
BLOCK: prev 2f5ba, self 1f805, height 1
BLOCK: prev 09620, self e75f8, height 6
BLOCK: prev e75f8, self 3a032, height 7
BLOCK: prev 2f247, self 980cd, height 15
INFO: current chain for node 6:
,height: 17BLOCK: prev 980cd, self 71145, height 16
BLOCK: prev 15add, self af79b, height 3
BLOCK: prev 09620, self e75f8, height 6
BLOCK: prev e75f8, self 3a032, height 7
BLOCK: prev 6e916, self 2e1e4, height 9
BLOCK: prev 2e1e4, self a9200, height 10
BLOCK: prev 6bb1d, self 5cd9c, height 13
BLOCK: prev FIRST, self 2f5ba, height 0
BLOCK: prev 2f5ba, self 1f805, height 1
BLOCK: prev af79b, self c49a3, height 4
BLOCK: prev a9200, self 3c149, height 11
BLOCK: prev 2f247, self 980cd, height 15
BLOCK: prev 1f805, self 15add, height 2
BLOCK: prev c49a3, self 09620, height 5
BLOCK: prev 5cd9c, self 2f247, height 14
BLOCK: prev 3a032, self 6e916, height 8
BLOCK: prev 3c149, self 6bb1d, height 12
BLOCK: prev 71145, self b518f, height 17
```

5.2 进攻成功测试结果 (3 良性 3 恶性)

```
Node Init: number 0
Node Init: number 1
Node Init: number 2
Node Init: number 3
Node Init: number 4
```

```
Node Init: number 5
Init Complete
MalNode start : number  5
Node start : number  0
Node start : number  2
MalNode start : number  3
MalNode start : number  4
Node start : number  1
INFO: node 0 has generated new block with hash d48b2
INFO: node 1 received INFO from 0
INFO: node 1 change the startBlock
INFO: node 2 received INFO from 0
INFO: node 2 change the startBlock
INFO: Malnode 3 has generated new block with hash c58c3
INFO: node 0 skipped malBlock
INFO: node 1 skipped malBlock
INFO: node 2 skipped malBlock
INFO: Malnode 4 change the startBlock
INFO: Malnode 5 change the startBlock
INFO: node 0 has generated new block with hash 4cda3
INFO: node 1 received INFO from 0
INFO: node 2 received INFO from 0
INFO: node 1 change the startBlock
INFO: node 2 change the startBlock
INFO: Malnode 4 has generated new block with hash 1838e
INFO: node 0 skipped malBlock
INFO: node 1 skipped malBlock
INFO: node 2 skipped malBlock
INFO: Malnode 3 change the startBlock
INFO: Malnode 5 change the startBlock
INFO: Malnode 3 has generated new block with hash 57344
INFO: Malnode 4 change the startBlock
INFO: Malnode 5 change the startBlock
INFO: node 0 skipped malBlock
INFO: node 1 skipped malBlock
INFO: node 2 skipped malBlock
INFO:ATTACK SUCCESS! current benign height: 2, mal height 3
INFO: ATTACKER block sent
INFO: node 0 received INFO from 3
INFO: node 1 received INFO from 3
INFO: node 2 received INFO from 3
INFO: ATTACKER block sent
INFO: node 1 received INFO from 3
INFO: node 2 received INFO from 3
INFO: node 0 received INFO from 3
INFO: ATTACKER block sent
INFO: node 0 received INFO from 3
INFO: node 0 change the startBlock
INFO: node 1 received INFO from 3
INFO: node 1 change the startBlock
INFO: node 2 received INFO from 3
INFO: node 2 change the startBlock
```

```
INFO: Malnode 5 has generated new block with hash 37046
INFO: node 2 skipped malBlock
INFO: Malnode 3 change the startBlock
INFO: Malnode 4 change the startBlock
INFO: node 0 skipped malBlock
INFO: node 1 skipped malBlock
INFO:ATTACK SUCCESS! current benign height: 3, mal height 4
INFO: ATTACKER block sent
INFO: node 0 received INFO from 5
INFO: node 1 received INFO from 5
INFO: node 2 received INFO from 5
INFO: ATTACKER block sent
INFO: node 1 received INFO from 5
INFO: node 2 received INFO from 5
INFO: node 0 received INFO from 5
INFO: ATTACKER block sent
INFO: node 2 received INFO from 5
INFO: node 0 received INFO from 5
INFO: node 1 received INFO from 5
INFO: ATTACKER block sent
INFO: node 0 received INFO from 5
INFO: node 0 change the startBlock
INFO: node 1 received INFO from 5
INFO: node 1 change the startBlock
INFO: node 2 received INFO from 5
INFO: node 2 change the startBlock
INFO: node 0 has generated new block with hash cadde
INFO: node 1 received INFO from 0
INFO: node 1 change the startBlock
INFO: node 2 received INFO from 0
INFO: node 2 change the startBlock
INFO: node 2 has generated new block with hash 05c31
INFO: node 1 received INFO from 2
INFO: node 1 change the startBlock
INFO: node 0 received INFO from 2
INFO: node 0 change the startBlock
INFO: node 1 has generated new block with hash c41cc
INFO: node 0 received INFO from 1
INFO: node 0 change the startBlock
INFO: node 2 received INFO from 1
INFO: node 2 change the startBlock
INFO: node 1 has generated new block with hash c9c6c
INFO: node 0 received INFO from 1
INFO: node 0 change the startBlock
INFO: node 2 received INFO from 1
INFO: node 2 change the startBlock
INFO: Malnode 4 has generated new block with hash eaa9d
INFO: node 2 skipped malBlock
INFO: Malnode 3 change the startBlock
INFO: Malnode 5 change the startBlock
INFO: node 0 skipped malBlock
INFO: node 1 skipped malBlock
```

```
INFO: Malnode 4 has generated new block with hash bc438
INFO: Malnode 5 change the startBlock
INFO: node 0 skipped malBlock
INFO: node 1 skipped malBlock
INFO: node 2 skipped malBlock
INFO: Malnode 3 change the startBlock
INFO: Malnode 5 has generated new block with hash 4584a
INFO: node 2 skipped malBlock
INFO: Malnode 3 change the startBlock
INFO: Malnode 4 change the startBlock
INFO: node 0 skipped malBlock
INFO: node 1 skipped malBlock
INFO: node 2 has generated new block with hash d0203
INFO: node 1 received INFO from 2
INFO: node 1 change the startBlock
INFO: node 0 received INFO from 2
INFO: node 0 change the startBlock
INFO: current chain for node 2:
,height: 9BLOCK: prev d48b2, self 4cda3, height 2
BLOCK: prev c58c3, self 1838e, height 2
BLOCK: prev 1838e, self 57344, height 3
BLOCK: prev 57344, self 37046, height 4
BLOCK: prev 37046, self cadde, height 5
BLOCK: prev c41cc, self c9c6c, height 8
BLOCK: prev 6fe5d, self d48b2, height 1
BLOCK: prev 6fe5d, self c58c3, height 1
BLOCK: prev cadde, self 05c31, height 6
BLOCK: prev 05c31, self c41cc, height 7
BLOCK: prev c9c6c, self d0203, height 9
BLOCK: prev FIRST, self 6fe5d, height 0
INFO: current chain for node 5:
,height: 7BLOCK: prev FIRST, self 6fe5d, height 0
BLOCK: prev 6fe5d, self c58c3, height 1
BLOCK: prev c58c3, self 1838e, height 2
BLOCK: prev 1838e, self 57344, height 3
BLOCK: prev 57344, self 37046, height 4
BLOCK: prev 37046, self eaa9d, height 5
BLOCK: prev eaa9d, self bc438, height 6
BLOCK: prev bc438, self 4584a, height 7
INFO: MalNode 5 exited
INFO: current chain for node 3:
,height: 7BLOCK: prev eaa9d, self bc438, height 6
BLOCK: prev bc438, self 4584a, height 7
BLOCK: prev FIRST, self 6fe5d, height 0
BLOCK: prev 6fe5d, self c58c3, height 1
BLOCK: prev c58c3, self 1838e, height 2
BLOCK: prev 1838e, self 57344, height 3
BLOCK: prev 57344, self 37046, height 4
BLOCK: prev 37046, self eaa9d, height 5
INFO: MalNode 3 exited
INFO: current chain for node 1:
,height: 9BLOCK: prev 37046, self cadde, height 5
```

```
BLOCK: prev 05c31, self c41cc, height 7
BLOCK: prev c41cc, self c9c6c, height 8
BLOCK: prev 6fe5d, self c58c3, height 1
BLOCK: prev c58c3, self 1838e, height 2
BLOCK: prev 1838e, self 57344, height 3
BLOCK: prev 57344, self 37046, height 4
BLOCK: prev cadde, self 05c31, height 6
BLOCK: prev FIRST, self 6fe5d, height 0
BLOCK: prev 6fe5d, self d48b2, height 1
BLOCK: prev d48b2, self 4cda3, height 2
BLOCK: prev c9c6c, self d0203, height 9
GROWTH RATE INFO: 9 blocks generated during last 10 seconds
INFO: current chain for node 0:
,height: 9BLOCK: prev c58c3, self 1838e, height 2
BLOCK: prev 1838e, self 57344, height 3
BLOCK: prev 57344, self 37046, height 4
BLOCK: prev cadde, self 05c31, height 6
BLOCK: prev 05c31, self c41cc, height 7
BLOCK: prev FIRST, self 6fe5d, height 0
BLOCK: prev d48b2, self 4cda3, height 2
BLOCK: prev 6fe5d, self c58c3, height 1
BLOCK: prev c9c6c, self d0203, height 9
BLOCK: prev 6fe5d, self d48b2, height 1
BLOCK: prev 37046, self cadde, height 5
BLOCK: prev c41cc, self c9c6c, height 8
INFO: current chain for node 4:
,height: 7BLOCK: prev 1838e, self 57344, height 3
BLOCK: prev 57344, self 37046, height 4
BLOCK: prev 37046, self eaa9d, height 5
BLOCK: prev eaa9d, self bc438, height 6
BLOCK: prev bc438, self 4584a, height 7
BLOCK: prev FIRST, self 6fe5d, height 0
BLOCK: prev 6fe5d, self c58c3, height 1
BLOCK: prev c58c3, self 1838e, height 2
INFO: MalNode 4 exited
```