

区块链防重放攻击白皮书

区块链防重放攻击白皮书.....	1
一、前言介绍.....	3
1、什么是重放攻击.....	3
2、区块链重放攻击防止	3
3、防重放攻击开源代码&license.....	3
1) 防重放攻击开源代码	3
2) license	3
二、环境搭建.....	3
1、比特币源码防重放修改	3
1) 签名源码修改原理.....	4
2) 签名源码修改源码.....	4
3) 硬分叉源码修改原理	4
4) 硬分叉源码修改源码	4
2、比特币源码环境搭建	4
1) 比特币源码编译准备命令	4
2) 比特币源码编译命令	4
4) 比特币源码安装命令	4
5) 配置私有链网络环境	4
6) 检测区块网络链连接是否正常	5
3、docker 运行环境技术使用	5
1) docker 镜像共享.....	5
2) 查看容器.....	5
3) 清空原有数据	6
4) 配置 docker 环境.....	6
5) docker 环境重置.....	6
6) docker 执行自动化脚本目录	7
三、防攻击验证测试.....	7
1、测试自动化脚本.....	7
1) docker 自动化脚本目录	8
2) 自动化测试脚本示例	8
3) 测试结果一览	9

2、测试流程及结果说明	9
1) 测试环境说明	9
2) 获取各节点主要原始数据	10
3) 脚本使用说明	11
4) 比特币现有程序节点间挖矿及交易	12
(1)节点 btcorgNode1 挖矿并确认	12
(2)btcorgNode1 向 btcorgNode2 交易 10 个比特币	14
(3)btcorgNode2 向 btcorgNode1 交易 5 个比特币	16
5) 比特币现有程序节点与比特币 2K 非防重放程序间挖矿及交易	17
(1)btcorgNode1 挖矿，确认之前的交易。	17
(2)btchardforkNode1 挖矿，确认之前的交易	17
(3)btcorgNode1 向 btchardforkNode1 转账 10，并挖矿确认	18
(4)btchardforkNode1 向 btcorgNode1 转账 5，并挖矿确认	19
(5)btcorgNode1 向 btchardforkNode1 发起 5 笔转账，并挖矿确认	20
(6)btchardforkNode1 向 btcorgNode1 发起 5 笔转账，并挖矿确认	21
6) 比特币 2K 防重放程序节点与比特币 2K 非防重放程序间挖矿及交易	22
(1)btchardforkNode1 挖矿 100	22
(2)btcnewNode1 挖矿 101	23
(3)btchardforkNode1 向 btcnewNode1 转账 10，并挖矿确认	24
(4)btcnewNode1 向 btchardforkNode1 转账 5，并挖矿确认	25
7) 比特币 2K 防重放程序节点间挖矿及交易	26
(1)btcnewNode1 挖矿 101	26
(2)btcnewNode1 向 btcnewNode2 转账 10，并挖矿确认	27
(3)btcnewNode2 向 btcnewNode1 转账 5，并挖矿确认	29
8) 比特币 2K 防重放程序节点和比特币现有程序间挖矿及交易	30
(1)btcorgNode1 挖矿 100	30
(2)btcnewNode1 挖矿 100	31
(3)btcorgNode1 向 btcnewNode1 转账 10，并挖矿确认	32
(4)btcnewNode1 向 btcorgNode1 转账 5，并挖矿确认	33
 三、总结	 34

一、前言介绍

本次区块链防重放攻击课题来源于 DACA 协会举办的清华大学 iCenter “区块链技术公开课(一期)”课题作业，其目的是解决即将发生的比特币分叉后可能发生重放攻击问题，为比特币社区提供一个可行的解决方案，代表比特币中国社区向全世界发声。

1、什么是重放攻击

重放攻击(Replay Attacks)又称重播攻击、回放攻击，是指攻击者发送一个目的主机已接收过的包，来达到欺骗系统的目的，主要用于身份认证过程，破坏认证的正确性。重放攻击可以由发起者，也可以由拦截并重发该数据的敌方进行。攻击者利用网络监听或者其他方式盗取认证凭据，之后再把它重新发给认证服务器。重放攻击在任何网络通过过程中都可能发生，是计算机世界黑客常用的攻击方式之一。

2、区块链重放攻击防止

本项目主要模拟区块链系统在硬分叉以后，如何防止原来区块链上的交易同步到新的区块链上。通过，改变签名的算法，达到防止重放攻击的目的。通过清华大学 icenter 老师们的悉心教导，通过将近 2 个月的学习，在比特币源码的基础上完成了防重放攻击 1.0 的开发。

3、防重放攻击开源代码&license

1) 防重放攻击开源代码

我们已经将防重放攻击的源码分享到 GitHub 上，地址为：<https://github.com/btcgroup2/bitcoin>

2) license

本项目按照 MIT license 协议。欢迎大家多多交流 具体请参考 <https://opensource.org/licenses/MIT>。

二、环境搭建

环境搭建主要分为三个主要的方面，首先是对比特币源码进行防重放攻击修改，其次是在服务器上对代码进行编译和部署，最后是采用 docker 技术实现多个服务的模拟，以达到模拟多个比特币系统节点的目的。

1、比特币源码防重放修改

1) 签名源码修改原理

我们同过修改比特币源代码的签名机制，这样比特币分叉后新链和旧链新产生的交易的是两个不同的签名机制，新链和旧链在验证数据的时候由于各自采用自己的机制进行验证，对方的机制验证不了，就达到了防止重放攻击的目的。

2) 签名源码修改源码

我们的核心修改机制是在原签名的基础上，再次取反，代码如下：

```
void negate(){
    for(int i=0;i<WIDTH;i++){
        data[i]=~data[i];
    }
}
```

位置是：src/uint256.h；其余代码详见：

<https://github.com/btcgroup2/bitcoin/commit/47a52fea8efe79539248ad72157d86ca5a6cf310>

3) 硬分叉源码修改原理

我通过设置区块大小，来模拟硬分叉，因为模拟环境产生大量的交易数据繁琐耗时，且意义不大。

4) 硬分叉源码修改源码

源码位置在：src/consensus/consensus.h，具体如下：

```
static const unsigned int MAX_BLOCK_BASE_SIZE = 1000000;
static const unsigned int MAX_BLOCK_BASE_SIZE = 2000 ;
```

2、比特币源码环境搭建

1) 比特币源码编译准备命令

```
./autogen.sh
```

```
./configure --with-incompatible-bdb
```

2) 比特币源码编译命令

```
make
```

4) 比特币源码安装命令

```
make install
```

5) 配置私有链网络环境

```
rpcuser=btc1
```

```
rpcpassword=xxl12345
addnode=60.205.162.88
addnode=47.94.165.9
whitelist=60.205.162.88
whitelist=47.94.165.9
```

6) 检测区块链连接是否正常

```
root@iZ2zegchn2k04hhikcn4yjZ:~# netstat -pant
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address          State
PID/Program name
cp      0      0 0.0.0.0:18444            0.0.0.0:*                LISTEN
17569/bitcoind
tcp      0      0 127.0.0.1:18332          0.0.0.0:*                LISTEN
17569/bitcoind
tcp      0      0 172.17.246.239:58241    60.205.162.88:18444     ESTABLISHED
17569/bitcoind
tcp6     0      0 :::18444                 :::*                     LISTEN
17569/bitcoind
比特币源码安装参考 http://blog.csdn.net/rion\_chen/article/details/51104727.
```

3、docker 运行环境技术使用

为了解决多节点的测试问题,采用当前流行的 docke 技术。著名的 Hyperledger 的 fabric 项目(由 IBM 主导的),就用了容器技术进行网络隔离。本次开发虚拟化 6 个节点(2 个 bitcoin 的源代码节点,2 个硬分叉节点和 2 个防攻击节点)

1) docker 镜像共享

```
docker pull xuxinlai2002/btcnew
docker pull xuxinlai2002/btchardfork
docker pull xuxinlai2002/btcorg
```

2) 查看容器

```
root@iZ2ze4wxzv9g5i5r69vu06Z:~/mydocker# docker ps
```

CONTAINER ID	IMAGE	COMMAND	
CREATED	STATUS	PORTS	NAMES
da5c88d83f3e	xuxinlai2002/btcnew	"sh -c 'bitcoind -reg'"	10 minutes ago
Up 10 minutes	18444/tcp	btnewNode2	
162954e0feac	xuxinlai2002/btcnew	"sh -c 'bitcoind -reg'"	10 minutes ago
Up 10 minutes	18444/tcp	btnewNode1	
2907e68ad502	xuxinlai2002/btchardfork	"sh -c 'bitcoind -reg'"	10 minutes ago
Up 10 minutes	18444/tcp	btchardforkNode2	
ab2ba80bff53	xuxinlai2002/btchardfork	"sh -c 'bitcoind -reg'"	10 minutes ago
Up 10 minutes	18444/tcp	btchardforkNode1	
84955fb307e8	xuxinlai2002/btcorg	"sh -c 'bitcoind -reg'"	10 minutes ago
Up 10 minutes	18444/tcp	btcorgNode2	
ed2d1223c275	xuxinlai2002/btcorg	"sh -c 'bitcoind -reg'"	10 minutes ago
Up 10 minutes	18444/tcp	btcorgNode1	

3) 清空原有数据

```
root@iZ2ze4wxzv9g5i5r69vu06Z:~/mydocker# cleanAll
da5c88d83f3e
162954e0feac
2907e68ad502
ab2ba80bff53
84955fb307e8
ed2d1223c275
```

4) 配置 docker 环境

```
root@iZ2ze4wxzv9g5i5r69vu06Z:~/mydocker# setAll
9581b304488f2d2b042d5f39b038e37a8666625c46eae02e0019ba7689d9fa01
7c476428e7807267ab169f32c4e57f73bf39e6506aa71453954c2afe00c30857
b1323bd91291ca7b8cf7057b32c72029af17f04bf0036c3bc5868ba096fdb443
1d35b593c37281677d3723f51eb08e6b72b7cba2eb304223a0f822c8578e8a39
2124409a8df4a52eddd1c7acc2a38251e2cd0701d7ee4e4eb725a8902feed141
e74fa0d9398c7d7732dc1726d45445737ac7b0d6f2cb2010b775c65846a90c74
```

5) docker 环境重置

```
root@iZ2ze4wxzv9g5i5r69vu06Z:~/mydocker# resetAll
/root/mydocker
e74fa0d9398c
2124409a8df4
1d35b593c372
b1323bd91291
7c476428e780
9581b304488f
e2cbc3d893942329ccdeb514eb97d116838a297443681b5c5f3cb11730c8181d
d95f254c75686e086c6d45827438c346e5166434704e6e2f51dbd4c40462ba21
58df1c5e832aac2463f3d6a28e81865677eac6986fe9c91b8812893c3c84bf67
01ae29ac4832b87fed5d865e38c57704708f98fa170eac5b93ba4ac0a0379d65
076938e94aca1109dc690639f3775b74a6def6a6edda092b4d666ccfcba7e5f
272e228f0a94e474595e1f789d118624cfb1c86cb35ad70e1c215719acc4ba42
```

6) docker 执行自动化脚本目录

```
root@iZ2ze4wxzv9g5i5r69vu06Z:~/mydocker/tools# ll
total 24
drwxr-xr-x  2 root root 4096 Jul 10 21:42 ./
drwxr-xr-x 10 root root 4096 Jul 10 21:04 ../
-rwxrwxrwx  1 root root  328 Jul 10 16:43 cleanAll*
-rwxrwxrwx  1 root root   31 Jul 10 15:34 resetAll*
-rwxrwxrwx  1 root root  294 Jul 10 16:37 setAll*
-rwxrwxrwx  1 root root  705 Jul  9 23:28 startNodes*
```

三、防攻击验证测试

分布式系统测试是一项比较繁琐的工作，为了在有限的时间内完成复制的测试，开发了自动化测试脚本，并且在 docker 的宿主机环境里，测试通过。这样可以提供测试效率，为以后的系统的持续集成打下基础

1、测试自动化脚本

1) docker 自动化脚本目录

```
root@iZ2ze4wxzv9g5i5r69vu06Z:~/mydocker/tests# ll
total 120
-rwxr-xr-x  1 root root  659 Jul 10 22:58 confirmtx*
-rwxr-xr-x  1 root root  667 Jul 10 23:29 confirmtx.save*
-rwxr-xr-x  1 root root  336 Jul 10 21:40 generate*
-rwxr-xr-x  1 root root  213 Jul 10 23:29 generate.save*
-rwxr-xr-x  1 root root  556 Jul 10 20:24 getblockchaininfo*
-rwxrwxrwx  1 root root  775 Jul 10 21:43 getinfo*
-rwxrwxrwx  1 root root  658 Jul 10 16:27 test11*
-rwxrwxrwx  1 root root  663 Jul 10 17:08 test12*
-rwxrwxrwx  1 root root  648 Jul 10 17:07 test13*
-rwxr-xr-x  1 root root  898 Jul 10 22:28 transaction*
-rwxr-xr-x  1 root root  256 Jul 10 23:29 transaction.save*
-rwxr-xr-x  1 root root  354 Jul 10 23:29 transaction.save.1*
-rwxr-xr-x  1 root root  559 Jul 10 23:29 transaction.save.2*
-rwxr-xr-x  1 root root  864 Jul 10 23:29 transaction.save.3*
```

2) 自动化测试脚本示例

```
imgs=("btcorg" "btchardfork" "btcnew")
ctns=("1" "2")
declare ctnNum=0
#test instruction
logInfo="transaction : send teansaction from $1 to $2 amount $3 "
echo $logInfo | tee tests/log/$4.log
address=`docker exec -it $2 bitcoin-cli -regtest getnewaddress`
echo "address: $address" |tee -a tests/log/$4.log
txid=`docker exec -it $1 bitcoin-cli -regtest sendtoaddress $address $3`
echo "txid: $txid"|tee -a tests/log/$4.log
for img in "${imgs[@]}"
do
    for ctn in "${ctns[@]}"
    do
```



```

logInfo="nodes: ${img}Node$ctn, transaction info"
echo $logInfo | tee -a tests/log/$4.log
docker exec -it ${img}Node$ctn bitcoin-cli -regtest gettransaction $txid >
temp.con
cat -v temp.con |tr -d "^M" |tee -a tests/log/$4.log
done
done
#docker exec -it $1 bitcoin-cli -regtest generate $2 > temp.con
#cat -v temp.con |tr -d "^M" |tee -a tests/generate.log

```

3) 测试结果一览

```

root@iZ2ze4wxzv9g5i5r69vu06Z:~/mydocker/tests/log# ll
-rw-r--r-- 1 root root 4941 Jul 11 00:41 confirmtx11.log
-rw-r--r-- 1 root root 7221 Jul 11 00:18 generate01.log
-rw-r--r-- 1 root root 3199 Jul 11 00:11 getinfo01.log
-rw-r--r-- 1 root root 3196 Jul 10 23:04 test11.log
-rw-r--r-- 1 root root 7221 Jul 10 23:04 test12.log
-rw-r--r-- 1 root root 3209 Jul 10 23:05 test13.log
-rw-r--r-- 1 root root 2449 Jul 10 23:07 test21.log
-rw-r--r-- 1 root root 4941 Jul 10 23:09 test25.log
-rw-r--r-- 1 root root 3250 Jul 10 23:10 test28.log
-rw-r--r-- 1 root root 1729 Jul 10 23:15 test31.log
-rw-r--r-- 1 root root 4941 Jul 10 23:16 test33.log
-rw-r--r-- 1 root root 3291 Jul 10 23:22 test37.log
-rw-r--r-- 1 root root 2449 Jul 11 00:19 transaction01.log

```

2、测试流程及结果说明

1) 测试环境说明

本次测试所使用环境为协会提供的服务器,服务器系统为 Linux,Ubuntu,64 位 ,为了使测试更加具有说服力 ,我们每个版本程序两个节点 ,采用 docker 模拟 6 个比特币节点 ,各节点详细数据如下表所示 :

节点名称	节点程序版本	docker container id
------	--------	---------------------

btccorgNode1	比特币现有程序	ed2d1223c275
btccorgNode2	比特币现有程序	84955fb307e8
btccnewNode1	比特币 2K 防重放程序	162954e0feac
btccnewNode2	比特币 2K 防重放程序	da5c88d83f3e
btchardforkNode1	比特币现有 2K 非防重放程序	ab2ba80bff53
btchardforkNode2	比特币现有 2K 非防重放程序	2907e68ad502

注：各节点 docker 信息详见第二章第三节第二小节。

2) 获取各节点主要原始数据

在测试之前，首先要获取各节点的原始数据，包括原始块数，余额，地址等等，这样做是为了对比之后的测试数据，已验证测试的正确性。具体信息在日志 test11.log 中，主要数据如下表所示：

节点名称	getinfo 指令主要信息	getaddressesbyaccount "" 指令主要信息	备注
btccorgNode1	"version": 149900, "protocolversion": 70015, "walletversion": 139900, "balance": 0.00000000, "blocks": 0, "timeoffset": 0, "connections": 5,	"n3VHpJYepNisre33mDz6 my2eHup877ya1"	通过 getinfo 指令获取链的主要信息，此处没有一一列出，详见日志文件。
btccorgNode2	"version": 149900, "protocolversion": 70015, "walletversion": 139900, "balance": 0.00000000, "blocks": 0, "timeoffset": 0, "connections": 9,	"n46NRxPNkVFgXHn7G myzD9bubt2gBZf4p"	
btccnewNode1	"version": 149900, "protocolversion": 70015, "walletversion": 139900, "balance": 0.00000000, "blocks": 0, "timeoffset": 0, "connections": 9,	"muzvG6LZE1byxbe9Dcre 9zjTQTr1YUGnE2"	
btccnewNode2	"version": 149900, "protocolversion": 70015,	"mmAx7BrNydCVdjf6K4y 29ozggJBfq1cRnt"	

	"walletversion": 139900, "balance": 0.00000000, "blocks": 0, "timeoffset": 0, "connections": 9,		
btchardforkNode1	"version": 149900, "protocolversion": 70015, "walletversion": 139900, "balance": 0.00000000, "blocks": 0, "timeoffset": 0, "connections": 9,	"n2HiY7xtbzB3YTbYLpbH9 oU2E5b2NEWvn1"	
btchardforkNode2	"version": 149900, "protocolversion": 70015, "walletversion": 139900, "balance": 0.00000000, "blocks": 0, "timeoffset": 0, "connections": 9,	"muHHu4sqY4QaGo57sm XSgVPEkcpcDxWo"	

3) 脚本使用说明

getinfo:查询所有节点的info

getinfo [日志文件名 (不用写.log)]

Eg.

getinfo getinfo11

generate:挖矿

generate [节点名] [块数] [日志文件名 (不用写.log)]

Eg.

generate btcorgNode1 101 generate12

transaction:交易

transaction [节点1] [节点2] [金额] [日志文件名 (不用写.log)]

Eg.

transaction btcorgNode1 btcorgNode2 10 transaction22

1 生成节点2交易地址

2 节点1向节点2发起交易

3 所有节点查询交易

confirmtx:确认交易

confirmtx [节点名] [日志文件名 (不用写.log)]

Eg.

```
confirmmtx btcorgNode1 confirmmtx11
```

1 挖矿1块打包交易

2 所有节点查询新打包区块

getblockhash:获取指定高度块hash

```
getblockhash [高度] [日志文件名 (不用写.log)]
```

Eg.

```
getblockhash 101 getblockhash101
```

getnodes:获取节点信息

```
getnodes [日志文件名 (不用写.log)]
```

Eg.

```
getnodes getnodes1
```

4) 比特币现有程序节点间挖矿及交易

(1)节点 **btcorgNode1** 挖矿并确认

该节点挖矿101个块 (在regtest模式下,该块之后有100个块,该块才被确认,发放挖矿报酬),脚本主要代码:

```
docker exec -it $1 bitcoin-cli -regtest generate $2 > temp.con
```

```
cat -v temp.con |tr -d "^M" |tee -a tests/log/$3.log
```

执行脚本指令:

```
generate btcorgNode1 101 test12
```

日志文件test12.log部分数据:

```
generate 101 blocks from btcorgNode1
```

```
[  
  "63521a7be8bb511d03b28948176d09d13f37e72e0b77a2cf83845c5299edd218",  
  "7f758cde534c277368e524dca6d50cac39379320a5eeb3b3390ea93585cc62c4",  
  ...96行...  
  "198e18cf357e59b3febc609248661a407d9e3bec0c72394aaf8130c817452d1f",  
  "66dc83c012e2694eebe512630f5a3e1611e6974e1497ab59f7e8bfbd8691929b"  
]
```

再次获取各节点数据,具体数据在日志 test13.log 中,主要数据如下表所示:

节点名称	getinfo 指令主要信息	getaddressesbyaccount ""	备注
------	----------------	--------------------------	----

		指令主要信息	
btccorgNode1	"version": 149900, "protocolversion": 70015, "walletversion": 139900, "balance": 50.00000000, "blocks": 101, "timeoffset": 0, "connections": 5,	"n3VHpJYepNisre33mDz6 my2eHup877ya1"	通过 getinfo 指令获取链 的主要信息， 此处没有一 一列出，详见 日志文件。
btccorgNode2	"version": 149900, "protocolversion": 70015, "walletversion": 139900, "balance": 0.00000000, "blocks": 101, "timeoffset": 0, "connections": 10,	"n46NRxPNkVFgXHn7G myzD9bubt2gBZf4p"	
btccnewNode1	"version": 149900, "protocolversion": 70015, "walletversion": 139900, "balance": 0.00000000, "blocks": 101, "timeoffset": 0, "connections": 9,	"muzvG6LZE1byxbe9Dcre 9zjTQTr1YUGnE2"	
btccnewNode2	"version": 149900, "protocolversion": 70015, "walletversion": 139900, "balance": 0.00000000, "blocks": 101, "timeoffset": 0, "connections": 9,	"mmAx7BrNydCVdjf6K4y 29ozggJBfq1cRnt"	
btchardforkNode1	"version": 149900, "protocolversion": 70015, "walletversion": 139900, "balance": 0.00000000, "blocks": 101, "timeoffset": 0, "connections": 9,	"n2HiY7xtbzB3YTbYLpbH9 oU2E5b2NEWvn1"	
btchardforkNode2	"version": 149900, "protocolversion": 70015, "walletversion": 139900, "balance": 0.00000000, "blocks": 101, "timeoffset": 0, "connections": 9,	"muHHu4sqY4QaGo57sm XSgVPEkcpcDxWo"	

可见,节点 btcorgNode1 所挖之矿均为创币交易块,由于创币交易没有签名,各节点均接收通过。

(2)btcorgNode1 向 btcorgNode2 交易 10 个比特币

btcorgNode1向btcorgNode2转账10个比特币,脚本主要代码:

```
txid=`docker exec -it $1 bitcoin-cli -regtest sendtoaddress $address $3`  
echo "txid: $txid"|tee -a tests/log/$4.log
```

执行脚本指令:

```
transaction btcorgNode1 btcorgNode2 10 test21
```

btcorgNode1打包交易,脚本主要代码:

```
blockid=`docker exec -it $1 bitcoin-cli -regtest generate 1`  
blockid="{blockid:6:64}"  
echo "block: $blockid"|tee -a tests/log/$2.log
```

执行脚本指令:

```
confirmtx btcorgNode1 test22
```

日志文件test21.log部分数据:

btcorgNode1:

```
"amount": -10.00000000,  
"fee": -0.00003840,  
"confirmations": 0,  
"trusted": true,  
"txid": "46985a452c6279f0cc6310b365ad39fe5ad449a01202bc673f7edaf484046339",  
"walletconflicts": [  
],  
"time": 1499750964,  
"timereceived": 1499750964,  
"bip125-replaceable": "no",  
"details": [  
  {  
    "account": "",  
    "address": "msV1hY8kbQmvgsHDWYsKPrHrYhnVBh4tQ4",  
    "category": "send",  
    "amount": -10.00000000,  
    "vout": 0,  
    "fee": -0.00003840,
```

```

        "abandoned": false
    }
],
btcorgNode2:
"amount": 10.00000000,
  "confirmations": 0,
  "trusted": false,
  "txid": "46985a452c6279f0cc6310b365ad39fe5ad449a01202bc673f7edaf484046339",
  "walletconflicts": [
],
"time": 1499750964,
"timereceived": 1499750964,
"bip125-replaceable": "no",
"details": [
  {
    "account": "",
    "address": "msV1hY8kbQmvgsHDWYsKPrHrYhnVBh4tQ4",
    "category": "receive",
    "amount": 10.00000000,
    "label": "",
    "vout": 0
  }
],

```

再次获取各节点数据，具体数据在日志 test23.log 中，主要数据如下表所示：

节点名称	getinfo 指令主要信息	getaddressesbyaccount "" 指令主要信息	备注
btcorgNode1	"balance": 89.99996160, "blocks": 102, "connections": 10,	"n3VHpJYepNisre33mDz6 my2eHup877ya1"	通过 getinfo 指令获取链的主要信息，此处没有一一列出，详见日志文件。
btcorgNode2	"balance": 10.00000000, "blocks": 102, "connections": 10,	"n46NRrxPNkVFgXHn7G myzD9bubt2gBZf4p"	
btcnewNode1	"balance": 0.00000000, "blocks": 101, "connections": 10,	"muzvG6LZE1byxbe9Dcre 9zjTQTr1YUGnE2"	

btcnewNode2	"balance": 0.00000000, "blocks": 101, "connections": 10,	"mmAx7BrNydCVdjf6K4y 29ozggJBfq1cRnt"	
btchardforkNode1	"balance": 0.00000000, "blocks": 102, "connections": 10,	"n2HiY7xtbzB3YTbYLpbH9 oU2E5b2NEWvn1"	
btchardforkNode2	"balance": 0.00000000, "blocks": 102, "connections": 10,	"muHHu4sqY4QaGo57sm XSgVPEkcpcDxWo"	

可见比特币现有程序节点的balance数据符合要求，btcorgNode1：

$50+50-0.00003840=89.99996160$ ，btcorgNode2:10；则btcorgNode1可以向btcorgNode2发起交易，同时btchardforkNode1，2两个节点也接受到了交易块，而btcnewNode1,2两个节点没有交易块，说明这两个节点已经与其他4各节点分叉。

(3) btcorgNode2 向 btcorgNode1 交易 5 个比特币

btcorgNode2 向 btcorgNode1 转账 5 个比特币：

transaction btcorgNode2 btcorgNode1 5 test31

btcorgNode2 打包交易：

confirmtx btcorgNode2 test32

再次获取各节点数据，具体数据在日志 test33.log 中，主要数据如下表所示：

节点名称	getinfo 指令主要信息	getaddressesbyaccount "" 指令主要信息	备注
btcorgNode1	"balance": 144.99996160, "blocks": 103, "connections": 10,	"n3VHpJYepNisre33mDz6 my2eHup877ya1" "mqrUYzjZy8biCsKiiGpSSJ yqV2LhcWFgoT",	通过 getinfo 指令获取链 的主要信息， 此处没有一 一列出，详见 日志文件。
btcorgNode2	"balance": 4.99995480, "blocks": 103, "connections": 10,	"n46NRrxPNkVFgXHn7G myzD9bubt2gBZf4p" "mgjj6JYP9wZtotU3ZsFFg 4YzrpmurAbaVw",	
btcnewNode1	"balance": 0.00000000, "blocks": 101, "connections": 10,	"muzvG6LZE1byxbe9Dcre 9zjTQTr1YUGnE2"	
btcnewNode2	"balance": 0.00000000, "blocks": 101, "connections": 10,	"mmAx7BrNydCVdjf6K4y 29ozggJBfq1cRnt"	
btchardforkNode1	"balance": 0.00000000, "blocks": 103,	"n2HiY7xtbzB3YTbYLpbH9 oU2E5b2NEWvn1"	

	"connections": 10,		
btchardforkNode2	"balance": 0.00000000, "blocks": 103, "connections": 10,	"muHHu4sqY4QaGo57sm XSgVPEkcpcDxWo"	

再次确认比特币现有程序节点可以交易，同时btchardforkNode1，2两个节点也接受到了交易块，而btcnewNode1,2两个节点没有交易块，说明这两个节点已经与其他4各节点分叉。

5) 比特币现有程序节点与比特币 2K 非防重放程序间挖矿及交易

(1)btccorgNode1 挖矿，确认之前的交易。

该节点挖矿 100 块，确认上一节中的交易，因为 regtest 规则原因，所以此处需要挖矿确认之前的交易，以便下面测试，脚本主要代码同上。

执行脚本指令：

```
generate btccorgNode1 100 test41
```

日志文件test41.log数据略。

再次获取各节点数据，具体数据在日志 test42.log 中，主要数据如下表所示：

节点名称	getinfo 指令主要信息	getaddressesbyaccount "" 指令主要信息	备注
btccorgNode1	"balance": 5095.00000000, "blocks": 203, "connections": 10,	"n3VHpJYepNisre33mDz6 my2eHup877ya1" "mqrUYzjZy8biCsKiiGpSSJ yqV2LhcWFgoT",	通过 getinfo 指令获取链 的主要信息， 此处没有一 一列出，详见 日志文件。
btccorgNode2	"balance":55.00000000, "blocks": 203, "connections": 10,	"n46NRrxPNkVFgXHn7G myzD9bubt2gBzf4p" "mgjj6JYP9wZtotU3ZsFFg 4YzrpmurAbaVw",	
btcnewNode1	"balance": 0.00000000, "blocks": 101, "connections": 10,	"muzvG6LZE1byxbe9Dcre 9zjTQTr1YUGnE2"	
btcnewNode2	"balance": 0.00000000, "blocks": 101, "connections": 10,	"mmAx7BrNydCVdjf6K4y 29ozggJBfq1cRnt"	
btchardforkNode1	"balance": 0.00000000, "blocks": 203, "connections": 10,	"n2HiY7xtbzB3YTbYlPbH9 oU2E5b2NEWvn1"	
btchardforkNode2	"balance": 0.00000000, "blocks": 203, "connections": 10,	"muHHu4sqY4QaGo57sm XSgVPEkcpcDxWo"	

(2)btchardforkNode1 挖矿，确认之前的交易

该节点挖矿 101 块，确认上一节中的交易，因为 regtest 规则原因，所以此处需要挖矿确认之前的交易，以便下面测试，再次获取各节点数据，具体数据在日志 test52.log 中，主要数据如下表所示：

节点名称	getinfo 指令主要信息	getaddressesbyaccount "" 指令主要信息	备注
btccorgNode1	"balance": 8745.00000000, "blocks": 304, "connections": 10,	"n3VHpJYepNisre33mDz6 my2eHup877ya1" "mqrUYzjZy8biCsKiiGpSSJ yqV2LhcWFgoT",	通过 getinfo 指令获取链的主要信息，此处没有一一列出，详见日志文件。
btccorgNode2	"balance": 10.00000000, "blocks": 304, "connections": 10,	"n46NRxPNkVFgXHn7G myzD9bubt2gBZf4p" "mgjj6JYP9wZtotU3ZsFFg 4YzrpmurAbaVw",	
btccnewNode1	"balance": 0.00000000, "blocks": 101, "connections": 10,	"muzvG6LZE1byxbe9Dcre 9zJTQTr1YUGnE2"	
btccnewNode2	"balance": 0.00000000, "blocks": 101, "connections": 10,	"mmAx7BrNydCVdjf6K4y 29ozggJBfq1cRnt"	
btchardforkNode1	"balance": 25.00000000, "blocks": 304, "connections": 10,	"n2HiY7xtbzB3YTbYlPbH9 oU2E5b2NEWvn1"	
btchardforkNode2	"balance": 0.00000000, "blocks": 304, "connections": 10,	"muHHu4sqY4QaGo57sm XSgVPEkcpcDxWo"	

注意此处由btchardforkNode1节点挖矿101，而得到报酬25，可知报酬已经减半了。

(3)btccorgNode1 向 btchardforkNode1 转账 10，并挖矿确认

btccorgNode1 向 btchardforkNode1 转账 10：

transaction btccorgNode1 btchardforkNode1 10 test61

btccorgNode1 打包交易：

confirmtx btccorgNode1 test62

再次获取各节点数据，具体数据在日志 test63.log 中，主要数据如下表所示：

节点名称	getinfo 指令主要信息	getaddressesbyaccount "" 指令主要信息	备注
btccorgNode1	"balance": 8734.99996160, "blocks": 305,	"n3VHpJYepNisre33mDz6 my2eHup877ya1"	通过 getinfo 指令获取链

	"connections": 10,	"mqrUYzjZy8biCsKiiGpSSJ yqV2LhcWFgoT",	的主要信息， 此处没有一 一列出，详见 日志文件。
btccorgNode2	"balance": 55.00000000, "blocks": 305, "connections": 10,	"n46NRrxPNkVFgXHn7G myzD9bubt2gBZf4p" "mgjj6JYP9wZtotU3ZsFFg 4YzrpmurAbaVw",	
btccnewNode1	"balance": 0.00000000, "blocks": 101, "connections": 10,	"muzvG6LZE1byxbe9Dcre 9zjTQTr1YUGnE2"	
btccnewNode2	"balance": 0.00000000, "blocks": 101, "connections": 10,	"mmAx7BrNydCVdjf6K4y 29ozggJBfq1cRnt"	
btchardforkNode1	"balance": 60.00000000, "blocks": 305, "connections": 10,	"n2HiY7xtbzB3YTbYLpbH9 oU2E5b2NEWvn1"	
btchardforkNode2	"balance": 0.00000000, "blocks": 305, "connections": 10,	"muHHu4sqY4QaGo57sm XSgVPEkcpcDxWo"	

由数据可知，由于此时区块<2k，btchardfork 接受区块，重放攻击成功。

(4)btchardforkNode1 向 btccorgNode1 转账 5，并挖矿确认

btchardforkNode1 向 btccorgNode1 转账 5：

transaction btchardforkNode1 btccorgNode1 5 test71

btchardforkNode1 打包交易，此时区块<2k：

confirmtx btchardforkNode1 test72

再次获取各节点数据，具体数据在日志 test73.log 中，主要数据如下表所示：

节点名称	getinfo 指令主要信息	getaddressesbyaccount "" 指令主要信息	备注
btccorgNode1	"balance": 8739.99996160, "blocks": 306, "connections": 10,	"n3VHpJYepNisre33mDz6 my2eHup877ya1" "mqrUYzjZy8biCsKiiGpSSJ yqV2LhcWFgoT",	通过 getinfo 指令获取链 的主要信息， 此处没有一 一列出，详见 日志文件。
btccorgNode2	"balance": 55.00000000, "blocks": 306, "connections": 10,	"n46NRrxPNkVFgXHn7G myzD9bubt2gBZf4p" "mgjj6JYP9wZtotU3ZsFFg 4YzrpmurAbaVw",	
btccnewNode1	"balance": 0.00000000, "blocks": 101,	"muzvG6LZE1byxbe9Dcre 9zjTQTr1YUGnE2"	

	"connections": 10,		
btcnewNode2	"balance": 0.00000000, "blocks": 101, "connections": 10,	"mmAx7BrNydCVdjf6K4y29ozggJBfq1cRnt"	
btchardforkNode1	"balance": 79.99996160, "blocks": 306, "connections": 10,	"n2HiY7xtbzB3YTbYlPbH9oU2E5b2NEWvn1"	
btchardforkNode2	"balance": 0.00000000, "blocks": 306, "connections": 10,	"muHHu4sqY4QaGo57smXSgVPEkcpcDxWo"	

可见，上一章节的结论再次验证

(5) btcorgNode1 向 btchardforkNode1 发起 5 笔转账，并挖矿确认

技术原理同上，此处不再过多叙述。

再次获取各节点数据，具体数据在日志 test811.log 中，主要数据如下表所示：

节点名称	getinfo 指令主要信息	getaddressesbyaccount "" 指令主要信息	备注
btcorgNode1	"balance": 8694.99960240, "blocks": 307, "connections": 10,	"n3VHpJYepNisre33mDz6my2eHup877ya1" "mqrUYzjZy8biCsKiiGpSSJyqV2LhcWFGOT", "mkELTQbVpvGhBC4sUW3aD9cCLmmDiC1PmE"	通过 getinfo 指令获取链的主要信息，此处没有一一列出，详见
btcorgNode2	"balance": 55.00000000, "blocks": 307, "connections": 10,	"n46NRxPNkVFgXHn7GmyzD9bubt2gBZf4p" "mgjj6JYP9wZtotU3ZsFFg4YzrpmurAbaVw",	
btcnewNode1	"balance": 0.00000000, "blocks": 101, "connections": 10,	"muzvG6LZE1byxbe9Dcre9zjTQTr1YUGnE2"	
btcnewNode2	"balance": 0.00000000, "blocks": 101, "connections": 10,	"mmAx7BrNydCVdjf6K4y29ozggJBfq1cRnt"	
btchardforkNode1	"balance": 149.99996160, "blocks": 307, "connections": 10,	"mgzYH88LXvn7LZFBNGHj8qooubck3Eag6y", "mj35BkwytxvbFw7P2cN98HQZELHaAHWKS", "mjHG3tBfpGJqPQuVVVErJsYpJrr9yd2AS", "mmW5TjvNnrCsJ8FtYJuruyMyBqmF1hkYA", "mpHpTt4sWy3BtxGDnCSJ96eagh7Y2wsxZ", "mqGUePwFV5KPsD32y46AZ52YWje2TxVE", "mrDpPirVKZNHkibSqu3aGKmXusWXgvPKZ", "mt2UJ28Jd97sn6tH11c5BxgFs6AwYHtK", "mtUfejmwqSSE3ZNmTx3kHbHRenuRn9eQV", "myv3EF2z37s6nKakzaHo5aBsX96JiJi7vY", "n2HiY7xtbzB3YTbYlPbH9oU2E5b2NEWvn1"	

btchardforkNode2	"balance": 0.00000000, "blocks": 307, "connections": 10,	"muHHu4sqY4QaGo57smXSgVPEkpcDxWo"	日志文件。
------------------	--	-----------------------------------	-------

(6)btchardforkNode1 向 btcorgNode1 发起 5 笔转账，并挖矿确认

技术原理同上，此处不再过多叙述。

再次获取各节点数据，具体数据在日志 test917.log 中，主要数据如下表所示：

节点名称	getinfo 指令主要信息	getaddressesbyaccount "" 指令主要信息	备注
btcorgNode1	"balance": 8814.99960240, "blocks": 308, "connections": 10,	"mgEyS1XX7uRa5SE2uRtZyc7oxBYV4Aq24B", "mh4FomgAg5YNbyy5ycaWXYpUiftBe4kHb", "miVEd6HhGXWLGmJ4WqBxhXqGwgscFKhEb", "miq8KSjWfVqUexwp5QVkjzjChAQEnQsJXK", "mjurkwfmxR7doj8ebGyNZvhn6a1pKqV6a", "mkELTQbVpvGhBC4sUW3aD9cCLmmDiC1PmE" "mmXN67LBa1JgTyWhsd6HYLQEvenwzSghi2", "moBFHuqeAD82pE4Vdu1wVSzLPQySa4fn", "moSndcivPDyb2YBnGBNPjQjC2SPSVUX", "mpE5UAHLXfkC9aVSWiZVTeyee1UkZX26by", "mqrUYzjZy8biCsKiiGpSSJyqV2LhcWFgoT", "mrvGfhYzvcRLHp2APEFuBFXYDktmdTJh", "msCb1xS8ekY6stPVXLTaob3w9ox6r1Z7d", "mv1b7BBSyGLXRDePsuTK8vLx7wtXN8bm", "mw4CVeD3JbmuLDzuerYmiuVt4cJrLJ6ZEu", "mx3LVC2twPvrsQoGF3RC4Tmw6a8kk4xYW", "mxVBfUGikPmxkgNrey1Aftmh7qkUvHUus", "n3VHpJYepNisre33mDz6my2eHup877ya1"	通过 geti nfo 指令 获取 链的 主要 信息， 此处 没有 一一 列出， 详见 日志 文件。
btcorgNode2	"balance": 55.00000000, "blocks": 308, "connections": 10,	"n46NRrxPNkVFgXHn7GmyzD9bubt2gBZf4p" "mgjj6JYP9wZtotU3ZsFFg4YzrpmurAbaVw",	
btcnewNode1	"balance": 0.00000000, "blocks": 101, "connections": 10,	"muzvG6LZE1byxbe9Dcre9zjTQTr1YUGnE2"	
btcnewNode2	"balance": 0.00000000, "blocks": 101, "connections": 10,	"mmAx7BrNydCVdjf6K4y29ozggJBfq1cRnt"	
btchardforkNode1	"balance": 54.99906720, "blocks": 308, "connections": 10,	"mgzYH88LXvn7LZFBNgHj8qooubcK3Eag6y", "mj35BkwyTXvbFw7P2cN98HQZeLHaAHWKs", "mjHG3tBfpGJqPQuVVVERjsYpJrr9yd2AS", "mmW5TjvNnrCsJ8FtYJuruyMyBqmF1hkYA", "mpHpTt4sWy3BtxGDnCSJ96eagh7Y2wsxZ", "mqGUePwFV5KPsD32y46AZ52YWje2TxVE",	

		"mrDpPirVKZNHkibSqu3aGKmXusWXgvPKZ", "mt2UJ28Jd97sn6tH11c5BxgFs6AwYHtK", "mtUfejmwqSSE3ZNmTx3kHbHRenURn9eQV", "myv3EF2z37s6nKakzaHo5aBsX96JiJi7vY", "n2HiY7xtbzB3YTbYlPbH9oU2E5b2NEWvn1"	
btchardforkNode2	"balance": 0.00000000, "blocks": 308, "connections": 10,	"muHHu4sqY4QaGo57smXSgVPEkpcDxWo"	

6) 比特币 2K 防重放程序节点与比特币 2K 非防重放程序间挖矿及交易

(1)btchardforkNode1 挖矿 100

技术原理同上，此处不再过多叙述。

再次获取各节点数据，具体数据在日志 test102.log 中，主要数据如下表所示：

节点名称	getinfo 指令主要信息	getaddressesbyaccount "" 指令主要信息	备注
btccorgNode1	"balance": 8840.00000000, "blocks": 408, "connections": 10,	"mgEyS1XX7uRa5SE2uRtZyc7oxBYV4Aq24B", "mh4FomgAg5YNbby5ycaWXYpUiftBe4kHb", "miVEd6HhGXWLGmJ4WqBxhXqGwgscFKhEb", "miq8KSjWfVqUexwp5QVkjzjChAQEnQsJXK", "mjurkwfmxR7doj8ebGyNZvhn6a1pKqV6a", "mkELTQbVpvGhBC4sUW3aD9cCLmmDiC1PmE", "mmXN67LBa1JgTyWhsd6HYLQEvenwzSghi2", "moBFHuqeAD82pE4Vdu1wVSzLPQySa4fn", "moSndcivPDyb2YBnGBNPjQjC2SPSVUX", "mpE5UAHLXfkC9aVSWiZVTeyee1UkZX26by", "mqrUYzjZy8biCsKiiGpSSJyqV2LhcWFgoT", "mrvGfhYzvcRLHp2APEFuBFXYDktmdTJh", "msCb1xS8ekY6stPVXLtaob3w9ox6r1Z7d", "mv1b7BBSYgVLXRDePsuTK8vLx7wtXN8bm", "mw4CVeD3JbmuLDzuerYmiuVt4cJrLJ6ZEu", "mx3LVC2twPvrsQoGF3RC4Tmw6a8kk4xYW", "mxVBfUGikPmxkgNrey1Aftmh7qkUvHUus", "n3VHpJYepNisre33mDz6my2eHup877ya1"	通过 geti nfo 指令 获取 链的 主要 信息， 此处 没有 一一 列出， 详见 日志 文
btccorgNode2	"balance": 55.00000000, "blocks": 408, "connections": 10,	"n46NRrxPNkVFgXHn7GmyzD9bubt2gBZf4p", "mgjj6JYP9wZtotU3ZsFFg4YzrpmurAbaVw",	
btccnewNode1	"balance": 0.00000000, "blocks": 101, "connections": 10,	"muzvG6LZE1byxbe9Dcre9zjTQTr1YUGnE2"	
btccnewNode2	"balance": 0.00000000, "blocks": 101, "connections": 10,	"mmAx7BrNydCVdjf6K4y29ozggJBfq1cRnt"	

btchardforkNode1	"balance": 2417.50000000, "blocks": 408, "connections": 10,	"mgzYH88LXvn7LZFBNGHj8qooubcK3Eag6y", "mj35BkwytXvbFw7P2cN98HQZeLHaAHWks", "mjHG3tBfpGJqPQuVVVErJsYpJrr9yd2AS", "mmW5TjvNnrcsj8FtYJuruymyBqmF1hkYA", "mpHpTt4sWy3BtxGDNCsJ96eagh7Y2wsxZ", "mqGUePwFV5KPsD32y46AZ52YWje2TxVE", "mrDpPirVKZNHkibSqu3aGKmXusWXgvPKZ", "mt2UJ28Jd97sn6tH11c5BxgFs6AwYHtK", "mtUfejmwqSSE3ZNmTx3kHbHRenuRn9eQV", "myv3EF2z37s6nKakzaHo5aBsX96JiJi7vY", "n2HiY7xtbzB3YTbYLPbH9oU2E5b2NEWvn1"	件。
btchardforkNode2	"balance": 0.00000000, "blocks": 408, "connections": 10,	"muHHu4sqY4QaGo57smXSgVPEkpcDxWo"	

(2)btccnewNode1 挖矿 101

技术原理同上，此处不再过多叙述。

再次获取各节点数据，具体数据在日志 test112.log 中，主要数据如下表所示：

节点名称	getinfo 指令主要信息	getaddressesbyaccount "" 指令主要信息	备注
btccorgNode1	"balance": 8840.00000000, "blocks": 408, "connections": 10,	"mgEyS1XX7uRa5SE2uRtZyc7oxBYV4Aq24B", "mh4FomgAg5YNbyy5ycaWXYpUiftBe4kHb", "miVEd6HhGXWLGmJ4WqBxhXqGwgsCFkHEb", "miq8KSjWfVqUexwp5QVkjzChAQEnQsJXK", "mjurkwfmxR7doj8ebGyNZvhn6a1pKqV6a", "mkELTQbVpvGhBC4sUW3aD9cCLmmDiC1PmE", "mmXN67LBa1JgTyWhsd6HYLQEvenwzSghi2", "moBFHuqeAD82pE4Vdu1wVSzLPQySa4fn", "moSndcvivPDyb2YBnGBNPjQjC2SPSVUX", "mpE5UAHLXfkC9aVSWiZVTeyee1UkZX26by", "mqrUYzjy8biCsKiiGpSSJyqV2LhcWFGOT", "mrvGfhYzvcRLHp2APEFuBFXYDktmdTJh", "msCb1xS8ekY6stPVXLTaob3w9ox6r1Z7d", "mv1b7BBSYgVLXRDePsuTK8vLx7wtXN8bm", "mw4CveD3JbmuLDzuerYmiuVt4cJrLJ6ZEu", "mx3LVC2twPvrsQoGF3RC4Tmw6a8kk4xYW", "mxVBfUGikPmxkgNrey1Aftmh7qkUvHUus", "n3VHpJYepNisre33mDz6my2eHup877ya1"	通过 geti nfo 指令 获取 链的 主要 信息， 此处 没有 一一 列出， 详
btccorgNode2	"balance": 55.00000000, "blocks": 408, "connections": 10,	"n46NRrxPNkVFgXHn7GmyzD9bubt2gBZf4p", "mgjj6JYP9wZtotU3ZsFFg4YzrprmurAbaVw",	
btccnewNode1	"balance": 50.00000000, "blocks": 202,	"muzvG6LZE1byxbe9Dcre9zjTQTr1YUGnE2"	

	"connections": 10,		见日志文件。
btcnwNode2	"balance": 0.00000000, "blocks": 202, "connections": 10,	"mmAx7BrNydCVdjf6K4y29ozggJBfq1cRnt"	
btchardforkNode1	"balance": 2417.50000000, "blocks": 408, "connections": 10,	"mgzYH88LXvn7LZFBNgHj8qooubcK3Eag6y", "mj35BkwytXvbFw7P2cN98HQZeLHaAHWks", "mjHG3tBfpGJqPQuVVVErJsYpJrr9yd2AS", "mmW5TjvNnrCsJ8FtYJuruymyBqmF1hkYA", "mpHpTt4sWy3BtxGDNCsJ96eagh7Y2wsxZ", "mqGUePwFV5KPsD32y46AZ52YWje2TxVE", "mrDpPirVKZNHkibSqu3aGKmXusWXgvPKZ", "mt2UJ28Jd97sn6tH11c5BxgFs6AwYHtK", "mtUfejmwqSSE3ZNmTx3kHbHRenRn9eQV", "myv3EF2z37s6nKakzaHo5aBsX96JiJi7vY", "n2HiY7xtbzB3YTbYLpbH9oU2E5b2NEWvn1"	
btchardforkNode2	"balance": 0.00000000, "blocks": 408, "connections": 10,	"muHHu4sqY4QaGo57smXSgVPEkpcDxWo"	

比特币2K防重放程序挖矿，因为已经分叉，所以这两个节点和其他四个节点的块传输阻塞。

(3)btchardforkNode1 向 btcnewNode1 转账 10，并挖矿确认

技术原理同上，此处不再过多叙述。

再次获取各节点数据，具体数据在日志 test123.log 中，主要数据如下表所示：

节点名称	getinfo 指令主要信息	getaddressesbyaccount "" 指令主要信息	备注
btccorgNode1	"balance": 8840.00000000, "blocks": 409, "connections": 10,	"mgEyS1XX7uRa5SE2uRtZyc7oxBYV4Aq24B", "mh4FomgAg5YNbby5ycaWXYpUiftBe4kHb", "miVEd6HhGXWLGmJ4WqBxhXqGwgscFKhEb", "miq8KSjWfVqUexwp5QVkjzjChAQEnQsJXK", "mjurkwfmxR7doj8ebGyNZvhn6a1pKqV6a", "mkELTQbVpvGhBC4sUW3aD9cCLmmDiC1PmE", "mmXN67LBa1JgTyWhsd6HYLQEvenwzSghi2", "moBFHuqeAD82pE4Vdu1wVSzLPQySa4fn", "moSNdcvivPDyb2YBnGBNPjQjC2SPSVUX", "mpE5UAHLXfkC9aVSWiZVTeyee1UkZX26by", "mqrUYzjZy8biCsKiiGpSSJyqV2LhcWFgoT", "mrvGfhYzvcRLHp2APEFuBFXYDktmdTJh", "msCb1xS8ekY6stPVXLtaob3w9ox6r1Z7d", "mv1b7BBSYgVLXRDePsuTK8vLx7wtXN8bm", "mw4CveD3JbmuLDzuerYmiuVt4cJrLJ6ZEu", "mx3LVC2twPvrsQoGF3RC4Tmw6a8kk4xYW", "mxVBfUGikPmxkgNrey1Aftmh7qkUvHUus", "n3VHPjYepNisre33mDz6my2eHup877ya1"	通过 getinfo 指令 获取 链的 主要 信息， 此处 没有

btccorgNode2	"balance": 55.00000000, "blocks": 409, "connections": 10,	"n46NRrxPNkVFgXHn7GmyzD9bubt2gBZf4p", "mgjj6JYP9wZtotU3ZsFFg4YzrpmurAbaVw",	一一列出, 详见日志文件。
btccnewNode1	"balance": 50.00000000, "blocks": 202, "connections": 10,	"mkq1TB1VQPiAXnJEybTFdWzpm6hDVbUu4", "muzvG6LZE1byxbe9Dcre9zjTQTr1YUGnE2"	
btccnewNode2	"balance": 0.00000000, "blocks": 202, "connections": 10,	"mmAx7BrNydCVdjf6K4y29ozggJBfq1cRnt"	
btchardforkNode1	"balance": 2419.99989560, "blocks": 409, "connections": 10,	"mgzYH88LXvn7LZFBNGHj8qooubcK3Eag6y", "mj35BkwytXvbFw7P2cN98HQZeLHaAHWks", "mjHG3tBfpGJqPQuVVVErJsYpJrr9yd2AS", "mmW5TjvNnrcsj8FtYJuruyMyBqmF1hkYA", "mpHpTt4sWy3BtxGDnCSJ96eagh7Y2wsxZ", "mqGUePwFV5KPsD32y46AZ52YWje2TxVE", "mrDpPirVKZNHkibSqu3aGKmXusWXgvPKZ", "mt2UJ28Jd97sn6tH11c5BxgFs6AwYHtK", "mtUfejmwqSSE3ZNmTx3kHbHRenuRn9eQV", "myv3EF2z37s6nKakzaHo5aBsX96JiJi7vY", "n2HiY7xtbzB3YTbYlPbH9oU2E5b2NEWvn1"	
btchardforkNode2	"balance": 0.00000000, "blocks": 409, "connections": 10,	"muHHu4sqY4QaGo57smXSgVPEkpcDxWo"	

由上面数据可知，btccnewNode不接受旧区块，节点区块数没有增加，balance也没有增加，防重放攻击成功。

(4)btccnewNode1 向 btchardforkNode1 转账 5，并挖矿确认

技术原理同上，此处不再过多叙述。

再次获取各节点数据，具体数据在日志 test133.log 中，主要数据如下表所示：

节点名称	getinfo 指令主要信息	getaddressesbyaccount "" 指令主要信息	备注
btccorgNode1	"balance": 8840.00000000, "blocks": 409, "connections": 10,	"mgEyS1XX7uRa5SE2uRtZyc7oxBYV4Aq24B", "mh4FomgAg5YNbyy5ycaWXYpUiftBe4kHb", "miVEd6HhGXWLGmJ4WqBxhXqGwgscFKhEb", "miq8KSjWfVqUexwp5QVkjzjChAQEnQsJXK", "mjurkwfmxR7doj8ebGyNZvhn6a1pKqV6a", "mkELTQbVpvGhBC4sUW3aD9cCLmmDiC1PmE", "mmXN67LBa1JgTyWhsd6HYLQEvenwzSghi2", "moBFHuqeAD82pE4Vdu1wVSzLPQySa4fn", "moSNdcvivPDyb2YBnGBNPjQjC2SPSVUX", "mpE5UAHLXfkC9aVSWiZVTeyee1UkZX26by", "mqrUYzjZy8biCsKiiGpSSJyqV2LhcWFGOT", "mrvGfhYzvcRLHp2APEFuBFXyDktmdTJh",	通过 getinfo 指令获取链的主要

		"msCb1xS8ekY6stPVXLTaob3w9ox6r1Z7d", "mv1b7BBSYgVLXRDePsuTK8vLx7wtXN8bm", "mw4CVeD3JbmuLDzuerYmiuVt4cJrLJ6ZEu", "mx3LVC2twPvrsQoGF3RC4Tmw6a8kk4xYW", "mxVBfUGikPmxkgNrey1Aftmh7qkUvHUus", "n3VHpJYepNisre33mDz6my2eHup877ya1"	信息，此处没有一一列出，详见日志文件。
btccorgNode2	"balance": 55.00000000, "blocks": 409, "connections": 10,	"n46NRrxPNkVFgXHn7GmyzD9bubt2gBZf4p", "mgjj6JYP9wZtotU3ZsFFg4YzrpmurAbaVw",	
btccnewNode1	"balance": 94.99996160, "blocks": 203, "connections": 10,	"mkq1TB1VQPiAXnJEybTFdWzpm6hDVbUu4", "muzvG6LZE1byxbe9Dcre9zjTQTr1YUGnE2"	
btccnewNode2	"balance": 0.00000000, "blocks": 203, "connections": 10,	"mmAx7BrNydCVdjf6K4y29ozggJBfq1cRnt"	
btchardforkNode1	"balance": 2419.99989560, "blocks": 409, "connections": 10,	"mgzYH88LXvn7LZFBNGHj8qooubcK3Eag6y", "mj35BkwytXvbFw7P2cN98HQZeLHaAHWks", "mjHG3tBfpGJqPQuVVVERJsYpJrr9yd2AS", "mmW5TjvNnrcsj8FtYJuruyMyBqmF1hkYA", "mpHpTt4sWy3BtxGDNCsJ96eagh7Y2wsxZ", "mqGUePwFV5KPsD32y46AZ52YWje2TxVE", "mrDpPirVKZNHkibSqu3aGKmXusWXgvPKZ", "mt2UJ28Jd97sn6tH11c5BxgFs6AwYHtK", "mtUfejmwqSSE3ZNmTx3kHbHRenuRn9eQV", "myv3EF2z37s6nKakzaHo5aBsX96JiJi7vY", "n2HiY7xtbzB3YTbYlPbH9oU2E5b2NEWvn1"	
btchardforkNode2	"balance": 0.00000000, "blocks": 409, "connections": 10,	"muHHu4sqY4QaGo57smXSgVPEkpcDxWo"	

再次验证上章节结论，btccnewNode 链长度增加，btchardforkNode 和 btccorgNode 不增加。

7) 比特币 2K 防重放程序节点间挖矿及交易

(1)btccnewNode1 挖矿 101

技术原理同上，此处不再过多叙述。

再次获取各节点数据，具体数据在日志 test142.log 中，主要数据如下表所示：

节点名称	getinfo 指令主要信息	getaddressesbyaccount "" 指令主要信息	备注
btccorgNode1	"balance": 8840.00000000, "blocks": 409, "connections": 10,	"mgEyS1XX7uRa5SE2uRtZyc7oxBYV4Aq24B", "mh4FomgAg5YNbyy5ycaWXYpUiftBe4kHb", "miVEd6HhGXWLGmJ4WqBxhXqGwgscFKhEb", "miq8KSjWfVqUexwp5QVkjzjChAQEnQsJXK", "mjurkwfmxR7doj8ebGyNZvhn6a1pKqV6a", "mkELTQbVpvGhBC4sUW3aD9cCLmmDiC1PmE"	通过 geti nfo 指令

		"mmXN67LBa1JgTyWhsd6HYLQEvenwzSghi2", "moBFHuqeAD82pE4Vdu1wVSzLPQySa4fn", "moSNdcvivPDyb2YBnGBNPjQjC2SPSVUX", "mpE5UAHLXfkC9aVSWiZVTeyee1UkZX26by", "mqrUYzjZy8biCsKiiGpSSJyqV2LhcWFgoT", "mrvGfhYzvcRLHp2APEFuBFXYDktmdTJh", "msCb1xS8ekY6stPVXLTaob3w9ox6r1Z7d", "mv1b7BBSYgVLXRDePsuTK8vLx7wtXN8bm", "mw4CVeD3JbmuLDzuerYmiuVt4cJrLJ6ZEu", "mx3LVC2twPvrsQoGF3RC4Tmw6a8kk4xYW", "mxVBfUGikPmxkgNrey1Aftmh7qkUvHUus", "n3VHpJYepNisre33mDz6my2eHup877ya1"	获取链的主要信息，此处没有一一列出，详见日志文件。
btccorgNode2	"balance": 55.00000000, "blocks": 409, "connections": 10,	"n46NRrxPNkVFgXHn7GmyzD9bubt2gBZf4p" "mgjj6JYP9wZtotU3ZsFFg4YzrpmurAbaVw",	
btccnewNode1	"balance": 3770.00000000, "blocks": 304, "connections": 10,	"mkq1TB1VQPiAXnJEybTFdWzpm6hDVbUu4", "muzvG6LZE1byxbe9Dcre9zjTQTr1YUGnE2"	
btccnewNode2	"balance": 0.00000000, "blocks": 304, "connections": 10,	"mmAx7BrNydCVdjf6K4y29ozggJBfq1cRnt"	
btcchardforkNode1	"balance": 2419.99989560, "blocks": 409, "connections": 10,	"mgzYH88LXvn7LZFBNGHj8qooubcK3Eag6y", "mj35BkwytXvbFw7P2cN98HQZeLHaAHWks", "mjHG3tBfpGJqPQuVVVERjsYpJrr9yd2AS", "mmW5TjvNnrcsj8FtYJuruyMyBqmF1hkYA", "mpHpTt4sWy3BtxGDncSJ96eagh7Y2wsxZ", "mqGUePwFV5KPsD32y46AZ52YWje2TxVE", "mrDpPirVKZNHkibSqu3aGKmXusWXgvPKZ", "mt2UJ28Jd97sn6tH11c5BxgFs6AwYHtK", "mtUfejmwqSSE3ZNmTx3kHbHRenURn9eQV", "myv3EF2z37s6nKakzaHo5aBsX96Jiji7vY", "n2HiY7xtbzB3YTbYLpbH9oU2E5b2NEWvn1"	
btcchardforkNode2	"balance": 0.00000000, "blocks": 409, "connections": 10,	"muHHu4sqY4QaGo57smXSgVPEkcpcDxWo"	

由数据可见，分叉后，btccnewNode 链长度增加，btcchardforkNode 和 btccorgNode 不增加

(2)btccnewNode1 向 btccnewNode2 转账 10，并挖矿确认

技术原理同上，此处不再过多叙述。

再次获取各节点数据，具体数据在日志 test153.log 中，主要数据如下表所示：

节点名称	getinfo 指令主要信息	getaddressesbyaccount ""	备
------	----------------	--------------------------	---

		指令主要信息	注
btccorgNode1	"balance": 8840.00000000, "blocks": 409, "connections": 10,	"mgEyS1XX7uRa5SE2uRtZyc7oxBYV4Aq24B", "mh4FomgAg5YNbyy5ycaWXYpUiftBe4kHb", "miVEd6HhGXWLGmJ4WqBxhXqGwgscFKhEb", "miq8KSjWfVqUexwp5QVkjzjChAQEnQsJXK", "mjurkwfmxR7doj8ebGyNZvhn6a1pKqV6a", "mkELTQbVpvGhBC4sUW3aD9cCLmmDiC1PmE", "mmXN67LBa1JgTyWhsd6HYLQEvenwzSghi2", "moBFHuqeAD82pE4Vdu1wVSzLPQySa4fn", "moSNdcvivPDyb2YBnGBNPjQjC2SPSVUX", "mpE5UAHLXfkC9aVSWiZVTeyee1UkZX26by", "mqrUYzjZy8biCsKiiGpSSJyqV2LhcWFgoT", "mrvGfhYzvcRLHp2APEFuBFXYDktmdTJh", "msCb1xS8ekY6stPVXLTaob3w9ox6r1Z7d", "mv1b7BBSYgVLXRDePsuTK8vLx7wtXN8bm", "mw4CVeD3JbmuLDzuerYmiuVt4cJrLJ6ZEu", "mx3LVC2twPvrsQoGF3RC4Tmw6a8kk4xYW", "mxVBfUGikPmxkgNrey1Aftmh7qkUvHUus", "n3VHpJYepNisre33mDz6my2eHup877ya1"	通过 getinfo 指令 获取 链的 主要 信息, 此处 没有 一一 列出, 详见 日志 文件。
btccorgNode2	"balance": 55.00000000, "blocks": 409, "connections": 10,	"n46NRrxPNkVFgXHn7GmyzD9bubt2gBZf4p", "mgjj6JYP9wZtotU3ZsFFg4YzrpmurAbaVw",	
btccnewNode1	"balance": 3784.99996160, "blocks": 305, "connections": 10,	"mkq1TB1VQPiAXnJEybTFdWzpm6hDVbUu4", "muzvG6LZE1byxbe9Dcre9zjTQTr1YUGnE2"	
btccnewNode2	"balance": 10.00000000, "blocks": 305, "connections": 10,	"mmAx7BrNydCVdfj6K4y29ozggJBfq1cRnt"	
btchardforkNode1	"balance": 2419.99989560, "blocks": 409, "connections": 10,	"mgzYH88LXvn7LZFBNGHj8qqoubcK3Eag6y", "mj35BkwytXvbFw7P2cN98HQZeLHaAHWks", "mjHG3tBfpGJqPQuVVVERjsYpJrr9yd2AS", "mmW5TjvNnrcsj8FtYJuruyMyBqmF1hkYA", "mpHpTt4sWy3BtxGDNCsJ96eagh7Y2wsxZ", "mqGUePwFV5KPsD32y46AZ52YWje2TxVE", "mrDpPirVKZNHkibSqu3aGKmXusWXgvPKZ", "mt2UJ28Jd97sn6tH11c5BxgFs6AwYHtK", "mtUfejmwqSSE3ZNmTx3kHbHRenuRn9eQV", "myv3EF2z37s6nKakzaHo5aBsX96JiJi7vY", "n2HiY7xtbzB3YTbYlPbH9oU2E5b2NEWvn1"	
btchardforkNode2	"balance": 0.00000000, "blocks": 409, "connections": 10,	"muHHu4sqY4QaGo57smXSgVPEkpcDxWo"	

由数据可见,分叉后,btccnewNode 链长度增加,btchardforkNode 和btccorgNode不增加,防重放

成功。

(3) btcnewNode2 向 btcnewNode1 转账 5，并挖矿确认

技术原理同上，此处不再过多叙述。

再次获取各节点数据，具体数据在日志 test163.log 中，主要数据如下表所示：

节点名称	getinfo 指令主要信息	getaddressesbyaccount "" 指令主要信息	备注
btccorgNode1	"balance": 8840.00000000, "blocks": 409, "connections": 10,	"mgEyS1XX7uRa5SE2uRtZyc7oxBYV4Aq24B", "mh4FomgAg5YNbby5ycaWXYpUiftBe4kHb", "miVEd6HhGXWLGmJ4WqBxhXqGwgscFKhEb", "miq8KSjWfVqUexwp5QVkjzjChAQEnQsJXK", "mjurkwfmxR7doj8ebGyNZvhn6a1pKqV6a", "mkELTQbVpvGhBC4sUW3aD9cCLmmDiC1PmE", "mmXN67LBa1JgTyWhsd6HYLQEvenwzSghi2", "moBFHuqeAD82pE4Vdu1wVSzLPQySa4fn", "moSndcivvPDyb2YBnGBNPjQjC2SPSVUX", "mpE5UAHLXfkC9aVSWiZVTeyee1UkZX26by", "mqrUYzjZy8biCskiiGpSSJyqV2LhcWFGOT", "mrvGfhYzvcRLHp2APEFuBFXYDktmdTJh", "msCb1xS8ekY6stPVXLtaob3w9ox6r1Z7d", "mv1b7BBSYgVLXRDePsuTK8vLx7wtXN8bm", "mw4CVeD3JbmULDzuerYmiuVt4cJrLJ6ZEu", "mx3LVC2twPvrsQoGF3RC4Tmw6a8kk4xYW", "mxVBfUGikPmxkgNrey1Aftmh7qkUvHUus", "n3VHpJYepNisre33mDz6my2eHup877ya1"	通过 geti nfo 指 令 获 取 链 的 主 要 信 息， 此 处 没 有 一 一 列 出， 详 见 日 志 文 件。
btccorgNode2	"balance": 55.00000000, "blocks": 409, "connections": 10,	"n46NRrxPNkVFgXHn7GmyzD9bubt2gBZf4p", "mgjj6JYP9wZtotU3ZsFFg4YzrpmurAbaVw",	
btcnewNode1	"balance": 3814.99996160, "blocks": 306, "connections": 10,	"mkq1TB1VQPiAXnJEybTFdWzpm6hDVbUu4", "muzvG6LZE1byxbe9Dcre9zjTQTr1YUGnE2", "n22F9DeejoS3baZwKoFW63SeB39W4xPSx"	
btcnewNode2	"balance": 4.99995480, "blocks": 306, "connections": 10,	"mmAx7BrNydCVdjf6K4y29ozggJBfq1cRnt", "n1Y7hQbotCPz4xpfYX6apoKEX9FuiWvv3q"	
btchardforkNode1	"balance": 2419.99989560, "blocks": 409, "connections": 10,	"mgzYH88LXvn7LZFBNGHj8qooubcK3Eag6y", "mj35BkwytXvbFw7P2cN98HQZeLHaAHWks", "mjHG3tBfpGJqPQuVVVerJsYpJrr9yd2AS", "mmW5TjvNnrcsj8FtYJuruyMyBqmF1hkYA", "mpHpTt4sWy3BtxGDNCsJ96eagh7Y2wsxZ", "mqGUePwFV5KPsD32y46AZ52YWje2TxVE", "mrDpPirVKZNHkibSqu3aGKmXusWXgvPKZ", "mt2UJ28Jd97sn6tH11c5BxgFs6AwYHtK",	

		"mtUfejmwqSSE3ZNmTx3kHbHRenRn9eQV", "myv3EF2z37s6nKakzaHo5aBsX96Ji7vY", "n2HiY7xtbzB3YTbYLpbH9oU2E5b2NEWvn1"	
btchardforkNode2	"balance": 0.00000000, "blocks": 409, "connections": 10,	"muHHu4sqY4QaGo57smXSgVPEkcpcDxWo"	

由数据可见，分叉后，btcnewNode 链长度增加，btchardforkNode 和btcorgNode不增加，防重放成功。

8) 比特币 2K 防重放程序节点和比特币现有程序间挖矿及交易

(1)btcorgNode1 挖矿 100

技术原理同上，此处不再过多叙述。

再次获取各节点数据，具体数据在日志 test172.log 中，主要数据如下表所示：

节点名称	getinfo 指令主要信息	getaddressesbyaccount "" 指令主要信息	备注
btcorgNode1	"balance": 8840.00000000, "blocks": 509, "connections": 10,	"mgEyS1XX7uRa5SE2uRtZyc7oxBYV4Aq24B", "mh4FomgAg5YNbby5ycaWXYpUiftBe4kHb", "miVEd6HhGXWLGmJ4WqBxhXqGwgscFKhEb", "miq8KSjWfVqUexwp5QVkjzjChAQEnQsJXK", "mjurkwfmxR7doj8ebGyNZvhn6a1pKqV6a", "mkELTQbVpVgHBC4sUW3aD9cCLmmDiC1PmE", "mmXN67LBa1JgTyWhsd6HYLQEvenwzSghi2", "moBFHuqeAD82pE4Vdu1wVSzLPQySa4fn", "moSNDcivvPDyb2YBnGBNPjQjC2SPSVUX", "mpE5UAHLXfkC9aVSWiZVTeyee1UkZX26by", "mqrUYzjZy8biCsKiiGpSSJyqV2LhcWFGOT", "mrvGfhYzvcRLHp2APEFuBFXYDktmdTJh", "msCb1xS8ekY6stPVXLtaob3w9ox6r1Z7d", "mv1b7BBSYgVLXRDePsuTK8vLx7wtXN8bm", "mw4CVeD3JbmuLDzuerYmiuVt4cJrLJ6ZEu", "mx3LVC2twPvrsQoGF3RC4Tmw6a8kk4xYW", "mxVBfUGikPmxkgNrey1Aftmh7qkUvHUus", "n3VHpJYepNisre33mDz6my2eHup877ya1"	通过 geti nfo 指令 获取 链的 主要 信息， 此处 没有 一一 列出， 详见 日志 文
btcorgNode2	"balance": 55.00000000, "blocks": 509, "connections": 10,	"n46NRrxPNkVFgXHn7GmyzD9bubt2gBZf4p", "mgjj6JYP9wZtotU3ZsFFg4YzrprmurAbaVw",	
btcnewNode1	"balance": 3814.99996160, "blocks": 306, "connections": 10,	"mkq1TB1VQPiAXnJEybTFdWzpm6hDVbUu4", "muzvG6LZE1byxbe9Dcre9zjTQTr1YUGnE2", "n22F9DeejoS3baZwKoFW63SeB39W4xPSx"	
btcnewNode2	"balance": 4.99995480, "blocks": 306,	"mmAx7BrNydCVdjf6K4y29ozggJBfq1cRnt", "n1Y7hQbotCPz4xpfYX6apoKEX9FuiWvW3q"	

	"connections": 10,		件。
btchardforkNode1	"balance": 3670.00000000, "blocks": 509, "connections": 10,	"mgzYH88LXvn7LZFBNGHj8qooubcK3Eag6y", "mj35BkwytXvbFw7P2cN98HQZeLHaAHWks", "mjHG3tBfpGJqPQuVVVrJsYpJrr9yd2AS", "mmW5TjvNnrscj8FtYJuruymyBqmF1hkYA", "mpHpTt4sWy3BtxGDNCsJ96eagh7Y2wsxZ", "mqGUePwFV5KPsD32y46AZ52YWje2TxVE", "mrDpPirVKZNHkibSqu3aGKmXusWXgvPKZ", "mt2UJ28Jd97sn6tH11c5BxgFs6AwYHtK", "mtUfejmwqSSE3ZNmTx3kHbHRenuRn9eQV", "myv3EF2z37s6nKakzaHo5aBsX96JiJi7vY", "n2HiY7xtbzB3YTbYlPbH9oU2E5b2NEWvn1"	
btchardforkNode2	"balance": 0.00000000, "blocks": 509, "connections": 10,	"muHHu4sqY4QaGo57smXSgVPEkpcDxWo"	

由数据可知，btcnewNode 链长度不增加，btchardforkNode 和 btcorgNode 增加

(2) btcnewNode1 挖矿 100

技术原理同上，此处不再过多叙述。

再次获取各节点数据，具体数据在日志 test182.log 中，主要数据如下表所示：

节点名称	getinfo 指令主要信息	getaddressesbyaccount "" 指令主要信息	备注
btcorgNode1	"balance": 8840.00000000, "blocks": 509, "connections": 10,	"mgEyS1XX7uRa5SE2uRtZyc7oxBYV4Aq24B", "mh4FomgAg5YNbyy5ycaWXYpUiftBe4kHb", "miVEd6HhGXWLGmJ4WqBxhXqGwgscFKhEb", "miq8KSjWfVqUexwp5QVkjzjChAQEnQsJXK", "mjurkwfmxR7doj8ebGyNZvhn6a1pKqV6a", "mkELTQbVpvGhBC4sUW3aD9cCLmmDiC1PmE", "mmXN67LBa1JgTyWhsd6HYLQEvenwzSghi2", "moBFHuqeAD82pE4Vdu1wVSzLPQySa4fn", "moSNdcvivPDyb2YBnGBNPjQjC2SPSVUX", "mpE5UAHLXfkC9aVSWiZVTeyee1UkZX26by", "mqrUYzjZy8biCsKiiGpSSJyqV2LhcWFgoT", "mrvGfhYzvcRLHp2APEFuBFXYDktmdTJh", "msCb1xS8ekY6stPVXLtaob3w9ox6r1Z7d", "mv1b7BBSYgVLXRDePsuTK8vLx7wtXN8bm", "mw4CveD3JbmuLDzuerYmiuVt4cJrLJ6ZEu", "mx3LVC2twPvrsQoGF3RC4Tmw6a8kk4xYW", "mxVBfUGikPmxkgNrey1Aftmh7qkUvHUus", "n3VHpJYepNisre33mDz6my2eHup877ya1"	通过 geti nfo 指令 获取 链的 主要 信息， 此处 没有 一一 列
btcorgNode2	"balance": 55.00000000, "blocks": 509, "connections": 10,	"n46NRrxPNkVFgXHn7GmyzD9bubt2gBZf4p", "mgjj6JYP9wZtotU3ZsFFg4YzrpmurAbaVw",	

btcnewNode1	"balance": 6215.00000000, "blocks": 406, "connections": 10,	"mkq1TB1VQPiAXnJEybTFdWzpm6hDVbUu4", "muzvG6LZE1byxbe9Dcre9zjTQTr1YUGnE2", "n22F9DeejoS3baZwKoFW63SeB39W4xPSx"	出， 详 见 日 志 文 件。
btcnewNode2	"balance": 17.50000000, "blocks": 406, "connections": 10,	"mmAx7BrNydCVdjf6K4y29ozggJBfq1cRnt", "n1Y7hQbotCPz4xpfYX6apoKEX9FuiWvv3q"	
btchardforkNode1	"balance": 3670.00000000, "blocks": 509, "connections": 10,	"mgzYH88LXvn7LZFBNGHj8qooubcK3Eag6y", "mj35BkwytXvbFw7P2cN98HQZeLHaAHWks", "mjHG3tBfpGJqPQuVVVERJsYpJrr9yd2AS", "mmW5TjvNnrcsj8FtYJuruymyBqmF1hkYA", "mpHpTt4sWy3BtxGDNCsJ96eagh7Y2wsxZ", "mqGUePwFV5KPsD32y46AZ52YWje2TxVE", "mrDpPirVKZNHkibSqu3aGKmXusWXgvPKZ", "mt2UJ28Jd97sn6tH11c5BxgFs6AwYHtK", "mtUfejmwwqSSE3ZNmTx3kHbHRenuRn9eQV", "myv3EF2z37s6nKakzaHo5aBsX96JiJi7vY", "n2HiY7xtbzB3YTbYLpbH9oU2E5b2NEWvn1"	
btchardforkNode2	"balance": 0.00000000, "blocks": 509, "connections": 10,	"muHHu4sqY4QaGo57smXSgVPEkpcDxWo"	

由数据可知，btcnewNode 链长度增加，btchardforkNode 和 btcorgNode 不增加

(3)btcorgNode1 向 btcnewNode1 转账 10，并挖矿确认

技术原理同上，此处不再过多叙述。

再次获取各节点数据，具体数据在日志 test193.log 中，主要数据如下表所示：

节点名称	getinfo 指令主要信息	getaddressesbyaccount "" 指令主要信息	备注
btcorgNode1	"balance": 8832.49985040, "blocks": 510, "connections": 10,	"mgEyS1XX7uRa5SE2uRtZyc7oxBYV4Aq24B", "mh4FomgAg5YNbyy5ycaWXYpUiftBe4kHb", "miVEd6HhGXWLGmJ4WqBxhXqGwsgcFKhEb", "miq8KSjWfVqUexwp5QVkjzjChAQEnQsJXK", "mjurkwfmxR7doj8ebGyNZvhn6a1pKqV6a", "mkELTQbVpvGhBC4sUW3aD9cCLmmDiC1PmE", "mmXN67LBa1JgTyWhsd6HYLQEvenwzSghi2", "moBFHuqeAD82pE4Vdu1wVSzLPQySa4fn", "moSndcivvPDyb2YBnGBNPjQjC2SPSVUX", "mpE5UAHLXfkC9aVSWiZVTeyee1UkZX26by", "mqrUYzjZy8biCskiiGpSSJyqV2LhcWFGOT", "mrvGfhYzvcRLHp2APEFuBFXYDktmdTJh", "msCb1xS8ekY6stPVXLtaob3w9ox6r1Z7d", "mv1b7BBSYgVLXRDePsuTK8vLx7wtXN8bm", "mw4CVeD3JbmuLDzuerYmiuVt4cJrLJ6ZEu", "mx3LVC2twPvrsQoGF3RC4Tmw6a8kk4xYW",	通 过 geti nfo 指 令 获 取 链 的 主 要 信 息， 此 处

		"mxVBfUGikPmxkgnrey1Aftmh7qkUvHUus", "n3VHpJYepNisre33mDz6my2eHup877ya1"	没有一一列出, 详见日志文件。
btccorgNode2	"balance": 55.00000000, "blocks": 510, "connections": 10,	"n46NRrxPNkVFGXHn7GmyzD9bubt2gBZf4p", "mgjj6JYP9wZtotU3ZsFFg4YzrpmurAbaVw",	
btccnewNode1	"balance": 6215.00000000, "blocks": 406, "connections": 10,	"mkq1TB1VQPiAXnJEybTFdWzpm6hDVbUu4", "muzvG6LZE1byxbe9Dcre9zjTQTr1YUGnE2", "n22F9DeejoS3baZwKoFW63SeB39W4xPSx"	
btccnewNode2	"balance": 17.50000000, "blocks": 406, "connections": 10,	"mmAx7BrNydCVdjf6K4y29ozggJBfq1cRnt", "n1Y7hQbotCPz4xpfYX6apoKEX9FuiWvw3q"	
btchardforkNode1	"balance": 3670.00000000, "blocks": 510, "connections": 10,	"mgzYH88LXvn7LZFBNGHj8qooubck3Eag6y", "mj35BkwytXvbFw7P2cN98HQZeLHaAHWks", "mjHG3tBfpGJqPQuVVVErJsYpJrr9yd2AS", "mmW5TjvNnrcsj8FtYJuruymyBqmF1hkYA", "mpHpTt4sWy3BtxGDnCSJ96eagh7Y2wsxZ", "mqGUePwFV5KPsD32y46AZ52YWje2TxVE", "mrDpPirVKZNHkibSqu3aGKmXusWXgvPKZ", "mt2UJ28Jd97sn6tH11c5BxgFs6AwYHtK", "mtUfejmwqSSE3ZNmTx3kHbHRenURn9eQV", "myv3EF2z37s6nKakzaHo5aBsX96JiJi7vY", "n2HiY7xtbzB3YTbYlPbH9oU2E5b2NEWvn1"	
btchardforkNode2	"balance": 0.00000000, "blocks": 510, "connections": 10,	"muHHu4sqY4QaGo57smXSgVPEkpcDxWo"	

由数据可知 在 tcorgNode1 打包交易后 ,btchardforkNode 和 btccorgNode 接收区块 ,btccnewNode 不接受, btccnewNode 链长度不增加, btchardforkNode 和 btccorgNode 增加, 防重放成功

(4)btccnewNode1 向 btccorgNode1 转账 5, 并挖矿确认

技术原理同上, 此处不再过多叙述。

再次获取各节点数据, 具体数据在日志 test203.log 中, 主要数据如下表所示:

节点名称	getinfo 指令主要信息	getaddressesbyaccount "" 指令主要信息	备注
btccorgNode1	"balance": 8832.49985040, "blocks": 510, "connections": 10,	"mgEyS1XX7uRa5SE2uRtZyc7oxBYV4Aq24B", "mh4FomgAg5YNbby5ycaWXYpUiftBe4kHb", "miVEd6HhGXWLGmJ4WqBxhXqGwgscFKhEb", "miq8KSjWfVqUexwp5QVkjzjChAQEnQsJXK", "mjurkwfmxR7doj8ebGyNZvhn6a1pKqV6a", "mkELTQbVpvGhBC4sUW3aD9cCLmmDiC1PmE", "mmXN67LBa1JgTyWhsd6HYLQEvenwzSghi2", "moBFHuqeAD82pE4Vdu1wVSzLPQySa4fn", "moSndcivPDyb2YBnGBNPjQjC2SPSVUX",	通过 getinfo 指令获取链

		"mpE5UAHLXfkC9aVSWiZVTeyee1UkZX26by", "mqrUYzjZy8biCsKiiGpSSJyqV2LhcWFgoT", "mrvGfhYzvcRLHp2APEFuBFXYDktmdTJh", "msCb1xS8ekY6stPVXLTaob3w9ox6r1Z7d", "mv1b7BBSYgVLXRDePsuTK8vLx7wtXN8bm", "mw4CVeD3JbmuLDzuerYmiuVt4cJrLJ6ZEu", "mx3LVC2twPvrsQoGF3RC4Tmw6a8kk4xYW", "mxVBfUGikPmxkgNrey1Aftmh7qkUvHUus", "n3VHpJYepNisre33mDz6my2eHup877ya1"	的主要信息，此处没有一一列出，详见日志文件。
btccorgNode2	"balance": 55.00000000, "blocks": 510, "connections": 10,	"n46NRrxPNkVfGXHn7GmyzD9bubt2gBZf4p" "mgjj6JYP9wZtotU3ZsFFg4YzrpmurAbaVw",	
btccnewNode1	"balance": 6222.49996160, "blocks": 407, "connections": 10,	"mkq1TB1VQPiAXnJEybTFdWzpm6hDVbUu4", "muzvG6LZE1byxbe9Dcre9zjTQTr1YUGnE2", "n22F9DeejoS3baZwKoFW63SeB39W4xPSx"	
btccnewNode2	"balance": 17.50000000, "blocks": 407, "connections": 10,	"mmAx7BrNydCVdjf6K4y29ozggJBfq1cRnt", "n1Y7hQbotCPz4xpfYX6apoKEX9FuiWvW3q"	
btcchardforkNode1	"balance": 3670.00000000, "blocks": 510, "connections": 10,	"mgzYH88LXvn7LZFBNGHj8qooubcK3Eag6y", "mj35BkwyTxbFw7P2cN98HQZeLHaAHWks", "mjHG3tBfpGJqPQuVVVErJsYpJrr9yd2AS", "mmW5TjvNnrcsj8FtYJuruyMyBqmF1hkYA", "mpHpTt4sWy3BtxGDnCSJ96eagh7Y2wsxZ", "mqGUePwFV5KPsD32y46AZ52YWje2TxVE", "mrDpPirVKZNHkibSqu3aGKmXusWXgvPKZ", "mt2UJ28Jd97sn6tH11c5BxgFs6AwYHtK", "mtUfejmwqSSE3ZNmTx3kHbHRenuRn9eQV", "myv3EF2z37s6nKakzaHo5aBsX96JiJi7vY", "n2HiY7xtbzB3YTbYLpbH9oU2E5b2NEWvn1"	
btcchardforkNode2	"balance": 0.00000000, "blocks": 510, "connections": 10,	"muHHu4sqY4QaGo57smXSgVPEkpcDxWo"	

再次验证防重放成功。

三、总结

本次开发由于时间比较短，另外团队成员的能力和精力有限，有很多不足之处。

比如，代码规范有待提高(注释最好用英文)，尚未完全模拟比特币真实环境，没有进行大规模的压力测试等待。 总之还有很多值得改进的地方。

但是，个人或者几个人的力量总是有限的，希望通过代码开源的形成，结合开源社区的力量。能够不断完善本项目，如有任何问题欢迎交流。 邮箱地址:xuxinlai2002@gmail.com

最后再次感谢 清华大学 icener 老师们的教导和支持！