

## B 组 · 防重放攻击实验测试报告

---

**B 组全体成员**

**2017 年 7 月 12 日**

模板修订履历

版本编号 或者记录编号	*变化状态	简要说明（变更内 容和变更范围）	日期	变更人	批准日期	批准人
V1.0	C					
V1.5	M					
V1.5	M					

\*变化状态：C——创建，A——增加，M——修改，D——删除

文档变更记录

日期	版本号	修订内容	修订人	审核人	批准人

目录

第一章 课题概述..... 4

1.1 课题名称..... 4

1.2 课题背景..... 4

1.3 课题目的..... 4

1.4 课题内容..... 4

1.5 测试环境..... 5

第二章 测试用例..... 8

2.1 测试方法..... 8

2.2 测试规划..... 8

2.3 测试结果..... 8

第三章 改进建议..... 18

# 第一章 课题概述

## 1.1 课题名称

区块链重放攻击解决方案——P2PKDH

## 1.2 课题背景

当区块链产生硬分叉后，就形成了两条链。由于这两条链上的地址和私钥生产算法相同，交易格式也完全相同，导致在其中一条链上的交易在另一条链上很可能是完全合法的。这就造成了区块链上发生了“重放攻击”。

## 1.3 课题目的

- A、认识比特币，了解比特币分叉产生的重放攻击原理及预防手段；
- B、学习重新编译比特币源码，了解编译比特币源码的基本方法和步骤；
- C、修改比特币源码，能够使用重新编译后的比特币钱包，模拟在区块链分叉时重放攻击双向失效的场景，加深对比特币原理的理解。

## 1.4 课题内容

(1) 提出 P2KHH 解决方案

(2) 修改 bitcoin 源码，代码实现方案：对交易格式进行修改,查阅代码，基于交易记录签名原理，对签名之前的交易 hash 值进行二次 hash 后再签名的方式，实现的效果：

- a)新的节点只认新节点产生的交易，旧节点只认旧节点产生的交易。
- b)新节点仍然可以使用旧节点中产生的 UTXO，新节点向旧节点转账不成功，旧节点向新节点地址转账也不成功。

基于以上分析，经过对代码进行查阅，在交易签名处理 interpreter.cpp 中增加如下代码：

```
33     uint256 hash = SignatureHash(scriptCode, *txTo, nIn, nHashType, amount, sigversion);
34
35     //modify by sholyn 2017.07.03 begin
36     CHashWriter ss(SER_GETHASH, 0);
37     ss << hash;
38     uint256 hash1 = ss.GetHash();
39     //modify by sholyn 2017.07.03 end
40
41     if (!key.Sign(hash1, vchSig))
42         return false;
```

在交易签名处理 sign.cpp 中增加如下代码:

```
1266     uint256 sighash = SignatureHash(scriptCode, *txTo, nIn, nHashType, amount, sigversion, this->txdata);
1267
1268     //modify by sholyn 2017.7.03 begin
1269     CHashWriter ss(SER_GETHASH, 0);
1270     ss << sighash;
1271     uint256 sighash1 = ss.GetHash();
1272     //modify by sholyn 2017.7.03 end
1273
1274     if (!VerifySignature(vchSig, pubkey, sighash1))
1275         return false;
```

3、搭建测试环境，模拟现实场景，设计了 3 种测试用例，验证了本方案可以有效抵御重放攻击。

## 1.5 测试环境

### 1、服务器 A:IP:47.94.199.129（北京）

old bitcoin path: /root/bitcoin

new bitcoind path: /home/sholyn/bitcoin

bitcoin config path: /root/.bitcoin/bitcoin.conf

bitcoin regtest data path: /root/.bitcoin/regtest

bitcoin config path: /root/.bitcoin/bitcoin.conf 具体配置如下:

```
#regtest=1
#dnsseed=0
#upnp=0

# always run a server, even with bitcoin-qt
#server=1

#listen on a port
#listen=1

# listen on different ports than default testnet
port=18000
rpcport=18334

#connect to node
#connect=172.104.124.159:18030
#connect=59.110.174.232:18020

# enable SSL for RPC server
#rpcssl=1

rpcallowip=0.0.0.0/0
rpcuser=bitcoinrpc
rpcpassword=sholyn@tinghua2017
```

## 2、服务器 B: IP:172.104.124.159（东京）

old bitcoin path: /root/bitcoin

new bitcoin path: /home/yj/bitcoin

bitcoin config path: /root/.bitcoin/bitcoin.conf

bitcoin regtest data path: /root/.bitcoin/regtest

bitcoin config path: /root/.bitcoin/bitcoin.conf 具体配置如下:

```
#regtest=1
#dnsseed=0
#upnp=0

# always run a server, even with bitcoin-qt
#server=1

#listen on a port
#listen=1

# listen on different ports than default testnet
port=18030
rpcport=18031

#connect to node
connect=47.94.199.129:18000

# enable SSL for RPC server
#rpcssl=1

rpccallowip=0.0.0.0/0

rpcuser=bitcoinrpc
rpcpassword=sholyn@tinghua2017
```

## 第二章 测试用例

### 2.1 测试方法

白盒测试

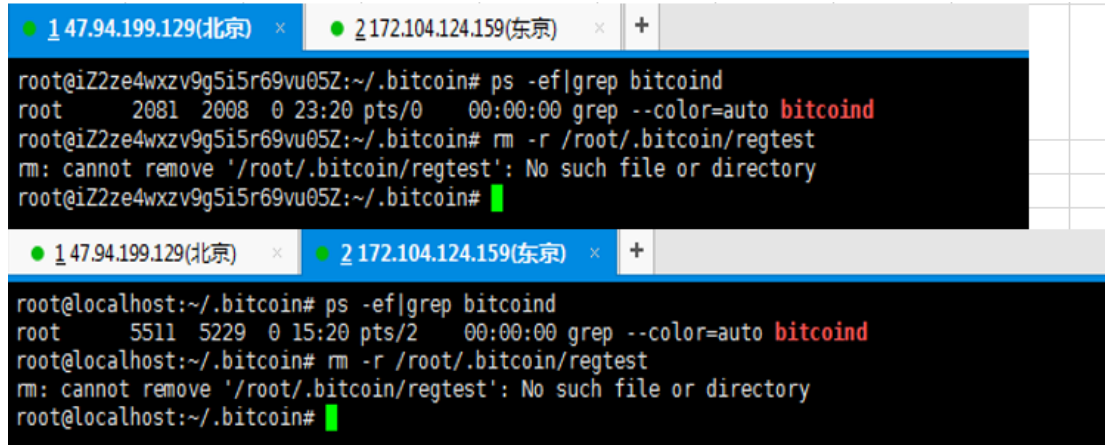
### 2.2 测试规划

测试项	测试步骤	描述/输入/操作	期望结果	真实结果	判断列	备注
1、两个旧节点之间转账测试	1) 服务器A上启动旧节点	/root/bitcoin/src/bitcoind -regtest -daemon				
	2) 服务器B上启动旧节点	/root/bitcoin/src/bitcoind -regtest -daemon				
	4) 服务器A上挖矿产生101个区块	/root/bitcoin/src/bitcoin-cli -regtest generate 101				
	5) 服务器A上查看UTXO	/root/bitcoin/src/bitcoin-cli -regtest getbalance	50	50	OK	
	6) 服务器B上查看UTXO	/root/bitcoin/src/bitcoin-cli -regtest getbalance	0	0	OK	
	7) 服务器B上生成新地址	/root/bitcoin/src/bitcoin-cli -regtest getnewaddress				
	8) 服务器A上向B中地址发动10BTC	/root/bitcoin/src/bitcoin-cli -regtest sendtoaddress XXX 10				
	9) 服务器A上查看UTXO	/root/bitcoin/src/bitcoin-cli -regtest getbalance	40	39.9999616	OK	此时A上余额已经扣除了。
	10) 服务器B上查看UTXO	/root/bitcoin/src/bitcoin-cli -regtest getbalance	0	0		B上还未到账，需要挖矿1次。
	11) 服务器A上挖矿产生1个区块	/root/bitcoin/src/bitcoin-cli -regtest generate 1				
	12) 服务器B上查看UTXO	/root/bitcoin/src/bitcoin-cli -regtest getbalance	10	10	OK	显示已经到账。
	13) 服务器A上查看UTXO	/root/bitcoin/src/bitcoin-cli -regtest getbalance	90	89.9999616	OK	显示已经到账。
	14) 服务器A上查看区块信息	/root/bitcoin/src/bitcoin-cli -regtest getinfo	102区块	102区块	OK	
	15) 服务器B上查看区块信息	/root/bitcoin/src/bitcoin-cli -regtest getinfo	102区块	102区块	OK	说明区块同步成功。
	16) 服务器A上停止旧节点	/root/bitcoin/src/bitcoin-cli -regtest stop				
	17) 服务器B上停止旧节点	/root/bitcoin/src/bitcoin-cli -regtest stop				
2、两个新节点之间转账测试	1) 服务器A上启动新节点	/home/sholyn/bitcoin/src/bitcoind -regtest -daemon				
	2) 服务器B上启动新节点	/home/yj/bitcoin/src/bitcoind -regtest -daemon				
	3) 服务器A上向B中地址发动10BTC	/home/sholyn/bitcoin/src/bitcoin-cli -regtest sendtoaddress XXX 10				
	4) 服务器A上挖矿产生1个区块	/home/sholyn/bitcoin/src/bitcoin-cli -regtest generate 1				
	5) 服务器A查看UTXO	/home/sholyn/bitcoin/src/bitcoin-cli -regtest getbalance	130	129.9999164	OK	
	6) 服务器B上查看UTXO	/home/yj/bitcoin/src/bitcoin-cli -regtest getbalance	20	20	OK	说明转账成功。
	7) 服务器A上查看区块信息	/home/sholyn/bitcoin/src/bitcoin-cli -regtest getinfo	103区块	103区块	OK	
	8) 服务器B上查看区块信息	/home/yj/bitcoin/src/bitcoin-cli -regtest getinfo	103区块	103区块	OK	说明区块同步成功。
	9) 服务器A上停止新节点	/home/sholyn/bitcoin/src/bitcoin-cli -regtest stop				
	10) 服务器B上停止新节点	/home/yj/bitcoin/src/bitcoin-cli -regtest stop				
3、新节点与旧节点之间转账测试	1) 服务器A上启动新节点	/home/sholyn/bitcoin/src/bitcoind -regtest -daemon				
	2) 服务器B上启动旧节点	/root/bitcoin/src/bitcoind -regtest -daemon				
	3) 服务器A上查看区块信息	/home/sholyn/bitcoin/src/bitcoin-cli -regtest getinfo	103区块	103区块		
	4) 服务器B上查看区块信息	/root/bitcoin/src/bitcoin-cli -regtest getinfo	103区块	103区块		
	5) 服务器A上向B中地址发动10BTC	/home/sholyn/bitcoin/src/bitcoin-cli -regtest sendtoaddress XXX 10				
	6) 服务器A上挖矿产生1个区块	/home/sholyn/bitcoin/src/bitcoin-cli -regtest generate 1				
	7) 服务器A上查看UTXO	/home/sholyn/bitcoin/src/bitcoin-cli -regtest getbalance	170	169.9998712	OK	
	8) 服务器B上查看UTXO	/root/bitcoin/src/bitcoin-cli -regtest getbalance	20	20	OK	说明转账未成功。
	9) 服务器A上查看区块信息	/home/sholyn/bitcoin/src/bitcoin-cli -regtest getinfo	104区块	104区块		
	10) 服务器B上查看区块信息	/root/bitcoin/src/bitcoin-cli -regtest getinfo	103区块	103区块	OK	说明区块未同步。
	11) 服务器A上生成新地址	/home/sholyn/bitcoin/src/bitcoin-cli -regtest getnewaddress				
	12) 服务器B上向A中地址发动10BTC	/root/bitcoin/src/bitcoin-cli -regtest sendtoaddress XXX 10				
	13) 服务器B上挖矿产生1个区块	/root/bitcoin/src/bitcoin-cli -regtest generate 1				
	14) 服务器B上查看UTXO	/root/bitcoin/src/bitcoin-cli -regtest getbalance	10	9.9999252	OK	
	15) 服务器A上查看UTXO	/home/sholyn/bitcoin/src/bitcoin-cli -regtest getbalance	170	169.9998712	OK	说明转账未成功。
	16) 服务器A上查看区块信息	/home/sholyn/bitcoin/src/bitcoin-cli -regtest getinfo	104区块	104区块		
	17) 服务器B上查看区块信息	/root/bitcoin/src/bitcoin-cli -regtest getinfo	104区块	104区块		目前并不能证明区块同步，需要继续在A或者B中挖矿
	18) 服务器B上挖矿产生10个区块	/root/bitcoin/src/bitcoin-cli -regtest generate 10				
	19) 服务器A上查看区块信息	/home/sholyn/bitcoin/src/bitcoin-cli -regtest getinfo	104	104	OK	说明区块未同步。
	20) 服务器B上查看区块信息	/root/bitcoin/src/bitcoin-cli -regtest getinfo	114	114		说明区块未同步。两个节点已经分差成功
	21) 服务器A上停止新节点	/home/sholyn/bitcoin/src/bitcoin-cli -regtest stop				
	22) 服务器B上停止旧节点	/root/bitcoin/src/bitcoin-cli -regtest stop				

### 2.3 测试结果



- 本次试验，我们使用 regtest 模式进行测试，为了防止干扰，首先分别移除各自对应的 regtest 目录。可以看到两个节点对应目录均已移除。



The image shows two terminal windows side-by-side. The top window is for node 1 at IP 47.94.199.129 (Beijing). The bottom window is for node 2 at IP 172.104.124.159 (Tokyo). Both windows show the command 'rm -r /root/.bitcoin/regtest' being executed, which results in the message 'rm: cannot remove '/root/.bitcoin/regtest': No such file or directory'.

```

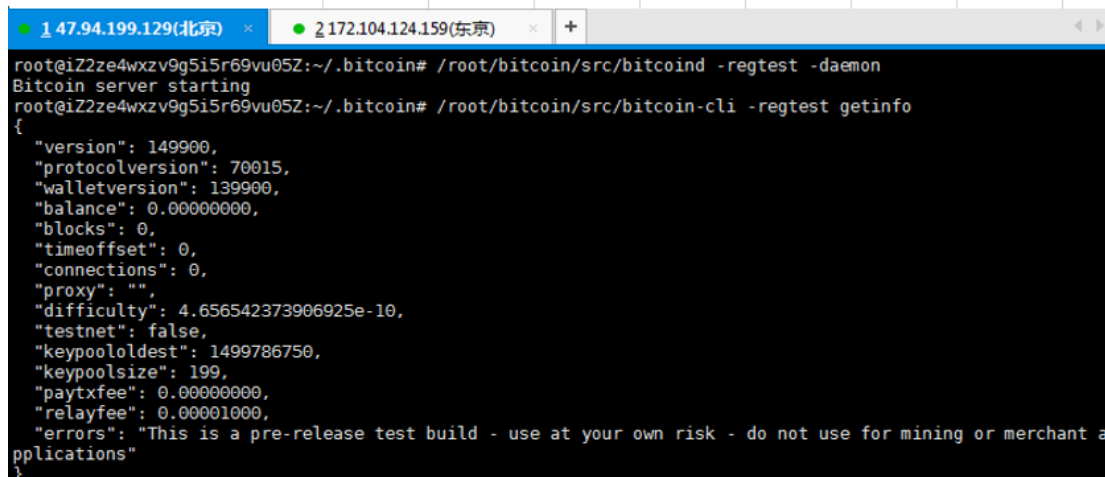
root@iZ2ze4wxzv9g5i5r69vu05Z:~/.bitcoin# ps -ef|grep bitcoind
root      2081  2008  0 23:20 pts/0    00:00:00 grep --color=auto bitcoind
root@iZ2ze4wxzv9g5i5r69vu05Z:~/.bitcoin# rm -r /root/.bitcoin/regtest
rm: cannot remove '/root/.bitcoin/regtest': No such file or directory
root@iZ2ze4wxzv9g5i5r69vu05Z:~/.bitcoin#

root@localhost:~/.bitcoin# ps -ef|grep bitcoind
root      5511  5229  0 15:20 pts/2    00:00:00 grep --color=auto bitcoind
root@localhost:~/.bitcoin# rm -r /root/.bitcoin/regtest
rm: cannot remove '/root/.bitcoin/regtest': No such file or directory
root@localhost:~/.bitcoin#

```

- 两个旧节点之间转账测试实验如下：

启动A并查看区块链信息



The image shows a terminal window for node 1 at IP 47.94.199.129 (Beijing). It shows the command '/root/bitcoin/src/bitcoind -regtest -daemon' being executed, followed by the output 'Bitcoin server starting'. Then, the command '/root/bitcoin/src/bitcoin-cli -regtest getinfo' is executed, resulting in a JSON object containing various node information.

```

root@iZ2ze4wxzv9g5i5r69vu05Z:~/.bitcoin# /root/bitcoin/src/bitcoind -regtest -daemon
Bitcoin server starting
root@iZ2ze4wxzv9g5i5r69vu05Z:~/.bitcoin# /root/bitcoin/src/bitcoin-cli -regtest getinfo
{
  "version": 149900,
  "protocolversion": 70015,
  "walletversion": 139900,
  "balance": 0.00000000,
  "blocks": 0,
  "timeoffset": 0,
  "connections": 0,
  "proxy": "",
  "difficulty": 4.656542373906925e-10,
  "testnet": false,
  "keypoololdest": 1499786750,
  "keypoolsize": 199,
  "paytxfee": 0.00000000,
  "relayfee": 0.00001000,
  "errors": "This is a pre-release test build - use at your own risk - do not use for mining or merchant applications"
}

```

启动B并查看区块信息

```

root@localhost:~/ .bitcoin# /root/bitcoin/src/bitcoind -regtest -daemon
Bitcoin server starting
root@localhost:~/ .bitcoin# /root/bitcoin/src/bitcoin-cli -regtest getinfo
{
  "version": 149900,
  "protocolversion": 70015,
  "walletversion": 139900,
  "balance": 0.00000000,
  "blocks": 0,
  "timeoffset": 0,
  "connections": 1,
  "proxy": "",
  "difficulty": 4.656542373906925e-10,
  "testnet": false,
  "keypoololdest": 1499786925,
  "keypoolsize": 199,
  "paytxfee": 0.00000000,
  "relayfee": 0.00001000,
  "errors": "This is a pre-release test build - use at your own risk - do not use for mining or merchant applications"
}

```

A产生101

```

root@iZ2ze4wxzv9g5i5r69vu05Z:~/ .bitcoin# /root/bitcoin/src/bitcoin-cli -regtest generate 101
[
  "4ca3b111ab907eadc077a06bd7255757387f104351120ae42d7cc6192f1de515",
  "72663f91fac8f6d0333a4e96bc2d28ded43fe0ad12ecc8e1dccc4e4dc0a1d110",
  "3b2c267a2aceeb3bfff65f13af3a8a2c6d999dbf6dd5cfe8b01e97af9573fe3",
  "4a0815e7369349052badb23115a5e959f2a33038d1cd84d215c86cf29459ebc1",
  "35d546fd57461e5fed26c0bb1c59ed763796e9aae11dd0a50589221baefd3605",
  "2fa151c741795d5ca720b7aedb730bdb65a0feab9a1a60589c7b8550f9ce867",
  "17a7d0999efbf20de45c7387df826fdd31fac6554a34b891fcf22fa43b08d1e",

```

A余额

```

root@iZ2ze4wxzv9g5i5r69vu05Z:~/ .bitcoin# /root/bitcoin/src/bitcoin-cli -regtest getbalance
50.00000000
root@iZ2ze4wxzv9g5i5r69vu05Z:~/ .bitcoin#

```

B余额

```

root@localhost:~/ .bitcoin# /root/bitcoin/src/bitcoin-cli -regtest getbalance
0.00000000
root@localhost:~/ .bitcoin#

```

B生成地址

```

root@localhost:~/ .bitcoin# /root/bitcoin/src/bitcoin-cli -regtest getnewaddress
mnFu8XinpNMLoLFhwZCrqypNGhTAzj7M6M
root@localhost:~/ .bitcoin#

```

A转B10

```

root@iZ2ze4wxzv9g5i5r69vu05Z:~/ .bitcoin# /root/bitcoin/src/bitcoin-cli -regtest sendtoaddress mnFu8XinpNMLoLFhwZCrqypNGhTAzj7M6M 10
cf6d7095f379b462e388bdeefcc9f4cd5bf493652b60daf8c45be00640fe6358
root@iZ2ze4wxzv9g5i5r69vu05Z:~/ .bitcoin#

```

A余额

```

root@iZ2ze4wxzv9g5i5r69vu05Z:~/ .bitcoin# /root/bitcoin/src/bitcoin-cli -regtest getbalance
39.99996160
root@iZ2ze4wxzv9g5i5r69vu05Z:~/ .bitcoin#

```

B余额

1 47.94.199.129(北京) × 2 172.104.124.159(东京) × +

```
root@localhost:~/bitcoin# /root/bitcoin/src/bitcoin-cli -regtest getbalance
0.00000000
root@localhost:~/bitcoin#
```

A挖矿

1 47.94.199.129(北京) × 2 172.104.124.159(东京) × +

```
root@iZ2ze4wxzv9g5i5r69vu05Z:~/bitcoin# /root/bitcoin/src/bitcoin-cli -regtest generate 1
[
  "03df4fb31a7912d23d68c47889aa1ec41657e217a81eb3a00132885a31da83f8"
]
root@iZ2ze4wxzv9g5i5r69vu05Z:~/bitcoin#
```

B余额

1 47.94.199.129(北京) × 2 172.104.124.159(东京) × +

```
root@localhost:~/bitcoin# /root/bitcoin/src/bitcoin-cli -regtest getbalance
10.00000000
root@localhost:~/bitcoin#
```

查看A信息

1 47.94.199.129(北京) × 2 172.104.124.159(东京) × +

```
root@iZ2ze4wxzv9g5i5r69vu05Z:~/bitcoin# /root/bitcoin/src/bitcoin-cli -regtest getinfo
{
  "version": 149900,
  "protocolversion": 70015,
  "walletversion": 139900,
  "balance": 89.99996160,
  "blocks": 102,
  "timeoffset": 0,
  "connections": 1,
  "proxy": "",
  "difficulty": 4.656542373906925e-10,
  "testnet": false,
  "keypoololdest": 1499786750,
  "keypoolsize": 199,
  "paytxfee": 0.00000000,
  "relayfee": 0.00001000,
  "errors": "This is a pre-release test build - use at your own risk - do not use for mining or merchant applications"
}
```

查看B信息

```

root@localhost:~/bitcoin# /root/bitcoin/src/bitcoin-cli -regtest getinfo
{
  "version": 149900,
  "protocolversion": 70015,
  "walletversion": 139900,
  "balance": 10.00000000,
  "blocks": 102,
  "timeoffset": 0,
  "connections": 1,
  "proxy": "",
  "difficulty": 4.656542373906925e-10,
  "testnet": false,
  "keypoololdest": 1499786925,
  "keypoolsize": 199,
  "paytxfee": 0.00000000,
  "relayfee": 0.00001000,
  "errors": "This is a pre-release test build - use at your own risk - do not use for mining or merchant applications"
}
root@localhost:~/bitcoin#

```

图中的服务器 A 的余额 89.9999616 与服务器 B 的余额 10.00000000 验证了两个旧节点之间转账成功。区块高度都是 102.表明测试通过。

A停止

```

root@iZ2ze4wxzv9g5i5r69vu05Z:~/bitcoin# /root/bitcoin/src/bitcoin-cli -regtest stop
Bitcoin server stopping
root@iZ2ze4wxzv9g5i5r69vu05Z:~/bitcoin#

```

B停止

```

root@localhost:~/bitcoin# /root/bitcoin/src/bitcoin-cli -regtest stop
Bitcoin server stopping
root@localhost:~/bitcoin#

```

➤ 两个新节点之间测试：

## A启动、查看区块信息

```

root@iZ2ze4wxzv9g5i5r69vu05Z:~/ .bitcoin# /home/sholyn/bitcoin/src/bitcoind -regtest -daemon
Bitcoin server starting
root@iZ2ze4wxzv9g5i5r69vu05Z:~/ .bitcoin# /home/sholyn/bitcoin/src/bitcoin-cli -regtest getinfo
{
  "version": 149900,
  "protocolversion": 70015,
  "walletversion": 139900,
  "balance": 89.99996160,
  "blocks": 102,
  "timeoffset": 0,
  "connections": 1,
  "proxy": "",
  "difficulty": 4.656542373906925e-10,
  "testnet": false,
  "keypoololdest": 1499832141,
  "keypoolsize": 199,
  "paytxfee": 0.00000000,
  "relayfee": 0.00001000,
  "errors": "This is a pre-release test build - use at your own risk - do not use for mining or merchant applications"
}

```

## B启动、查看区块信息

```

root@localhost:~/ .bitcoin# /home/yj/bitcoin/src/bitcoind -regtest -daemon
Bitcoin server starting
root@localhost:~/ .bitcoin# /home/yj/bitcoin/src/bitcoin-cli -regtest getinfo
{
  "version": 149900,
  "protocolversion": 70015,
  "walletversion": 139900,
  "balance": 10.00000000,
  "blocks": 102,
  "timeoffset": 0,
  "connections": 1,
  "proxy": "",
  "difficulty": 4.656542373906925e-10,
  "testnet": false,
  "keypoololdest": 1499832144,
  "keypoolsize": 199,
  "paytxfee": 0.00000000,
  "relayfee": 0.00001000,
  "errors": "This is a pre-release test build - use at your own risk - do not use for mining or merchant applications"
}

```

## A给B转账10、挖矿1个块、查看余额、查看区块信息

```

root@iZ2ze4wxzv9g5i5r69vu05Z:~/ .bitcoin# /home/sholyn/bitcoin/src/bitcoin-cli -regtest sendtoaddress mtmDRJfncn63pK7y8TWtdHTCDZAFDbc8Ci 10
12ab3e3d74aea62c96dfe2539c9208775fc9f1d03a53e03d2eaa05d74ef2f61a
root@iZ2ze4wxzv9g5i5r69vu05Z:~/ .bitcoin# /home/sholyn/bitcoin/src/bitcoin-cli -regtest generate 1
[
  "4d4997c23f3d0c8ea547c487762dba72e29d2a64c42bde4d8ed9b15c4b186cdf"
]
root@iZ2ze4wxzv9g5i5r69vu05Z:~/ .bitcoin# /home/sholyn/bitcoin/src/bitcoin-cli -regtest getbalance
129.99991640
root@iZ2ze4wxzv9g5i5r69vu05Z:~/ .bitcoin# /home/sholyn/bitcoin/src/bitcoin-cli -regtest getinfo
{
  "version": 149900,
  "protocolversion": 70015,
  "walletversion": 139900,
  "balance": 129.99991640,
  "blocks": 103,
  "timeoffset": 0,
  "connections": 1,
  "proxy": "",
  "difficulty": 4.656542373906925e-10,
  "testnet": false,
  "keypoololdest": 1499832141,
  "keypoolsize": 199,
  "paytxfee": 0.00000000,
  "relayfee": 0.00001000,
  "errors": "This is a pre-release test build - use at your own risk - do not use for mining or merchant applications"
}

```

B查看区块信息

```

1 47.94.199.129(北京) × 2 172.104.124.159(东京) × +
root@localhost:~/bitcoin# /home/yj/bitcoin/src/bitcoin-cli -regtest getinfo
{
  "version": 149900,
  "protocolversion": 70015,
  "walletversion": 139900,
  "balance": 20.00000000,
  "blocks": 103,
  "timeoffset": 0,
  "connections": 1,
  "proxy": "",
  "difficulty": 4.656542373906925e-10,
  "testnet": false,
  "keypoololdest": 1499832144,
  "keypoolsize": 199,
  "paytxfee": 0.00000000,
  "relayfee": 0.00001000,
  "errors": "This is a pre-release test build - use at your own risk - do not use for mining or merchant applications"
}

```

图中的服务器 A 的余额 129.99991640，与服务器 B 的余额 20.00000000 验证了新节点服

务器 A 与新节点服务器 B 之间转账成功。区块高度都是 103 表明测试通过。

A停止

```

1 47.94.199.129(北京) × 2 172.104.124.159(东京) × +
root@iZ2ze4wxzv9g5i5r69vu05Z:~/bitcoin# /root/bitcoin/src/bitcoin-cli -regtest stop
Bitcoin server stopping
root@iZ2ze4wxzv9g5i5r69vu05Z:~/bitcoin#

```

B停止

```

1 47.94.199.129(北京) × 2 172.104.124.159(东京) × +
root@localhost:~/bitcoin# /root/bitcoin/src/bitcoin-cli -regtest stop
Bitcoin server stopping
root@localhost:~/bitcoin#

```

➤ 新旧节点之间转账测试：

A启动、节点信息

```

1 47.94.199.129(北京) × 2 172.104.124.159(东京) × +
root@iZ2ze4wxzv9g5i5r69vu05Z:~/bitcoin# /home/sholyn/bitcoin/src/bitcoind -regtest -daemon
Bitcoin server starting
root@iZ2ze4wxzv9g5i5r69vu05Z:~/bitcoin# /home/sholyn/bitcoin/src/bitcoin-cli -regtest getinfo
{
  "version": 149900,
  "protocolversion": 70015,
  "walletversion": 139900,
  "balance": 129.99991640,
  "blocks": 103,
  "timeoffset": 0,
  "connections": 1,
  "proxy": "",
  "difficulty": 4.656542373906925e-10,
  "testnet": false,
  "keypoololdest": 1499832141,
  "keypoolsize": 199,
  "paytxfee": 0.00000000,
  "relayfee": 0.00001000,
  "errors": "This is a pre-release test build - use at your own risk - do not use for mining or merchant applications"
}

```



A转账B、挖矿1个块、查看余额、查看节点信息

```

root@iZ2ze4wxzv9g5i5r69vu05Z:~/bitcoin# /home/sholyn/bitcoin/src/bitcoin-cli -regtest sendtoaddress mtmDRJfncn63pK7y8TWtCDZAFDbc8Ci 10
09dff07af3819579b4865b9a708643e05d59644890143835a8f019c603dd8afc
root@iZ2ze4wxzv9g5i5r69vu05Z:~/bitcoin# /home/sholyn/bitcoin/src/bitcoin-cli -regtest generate 1
[
  "7dd21fe601603d70ecbbec281c730cbc989d494642f1f4fc7597d9e2c0ac507f"
]
root@iZ2ze4wxzv9g5i5r69vu05Z:~/bitcoin# /home/sholyn/bitcoin/src/bitcoin-cli -regtest getbalance
169.99987120
root@iZ2ze4wxzv9g5i5r69vu05Z:~/bitcoin# /home/sholyn/bitcoin/src/bitcoin-cli -regtest getinfo
{
  "version": 149900,
  "protocolversion": 70015,
  "walletversion": 139900,
  "balance": 169.99987120,
  "blocks": 104,
  "timeoffset": 0,
  "connections": 1,
  "proxy": "",
  "difficulty": 4.656542373906925e-10,
  "testnet": false,
  "keypoololdest": 1499832141,
  "keypoolsize": 199,
  "paytxfee": 0.00000000,
  "relayfee": 0.00001000,
  "errors": "This is a pre-release test build - use at your own risk - do not use for mining or merchant applications"
}

```

A日志

```

2017-07-12 04:18:02 receive version message: /Satoshi:0.14.99/: version 70015, blocks=103, us=47.94.199.129:18000, peer=0
2017-07-12 04:18:02 Leaving InitialBlockDownload (latching to false)
2017-07-12 04:18:40 Adding fixed seed nodes as DNS doesn't seem to be available.
2017-07-12 04:19:39 keypool added key 206, size=200, internal=0
2017-07-12 04:19:39 keypool reserve 103
2017-07-12 04:19:39 Fee Calculation: Fee:4520 Bytes:226 Tgt:6 (requested 6) Reason:"Fallback fee" Decay 0.00000: Estimation: (-1 - -1)
-nan% 0.0/(0.0 0 mem 0.0 out) Fail: (-1 - -1) -nan% 0.0/(0.0 0 mem 0.0 out)
2017-07-12 04:19:39 CommitTransaction:
CTransaction(hash=09dff07af3, ver=2, vin.size=1, vout.size=2, nLockTime=103)
  CTxIn(COutPoint(12ab3e3d74, 1), scriptSig=483045022100c001d2583ce3, nSequence=4294967294)
    CScriptWitness()
      CTxOut(nValue=10.00000000, scriptPubKey=76a914914c159a82c698824ab3f3ce)
      CTxOut(nValue=19.99987120, scriptPubKey=76a914cbab7c92cc4647606cbf7676)
2017-07-12 04:19:39 keypool keep 103
2017-07-12 04:19:39 AddToWallet 09dff07af3819579b4865b9a708643e05d59644890143835a8f019c603dd8afc new
2017-07-12 04:19:39 AddToWallet 09dff07af3819579b4865b9a708643e05d59644890143835a8f019c603dd8afc
2017-07-12 04:19:39 Relaying wtx 09dff07af3819579b4865b9a708643e05d59644890143835a8f019c603dd8afc
2017-07-12 04:19:41 receive version message: /Satoshi:0.14.99/: version 70015, blocks=103, us=47.94.199.129:18000, peer=1
2017-07-12 04:19:49 keypool added key 207, size=200, internal=1
2017-07-12 04:19:49 keypool reserve 5
2017-07-12 04:19:49 CreateNewBlock(): total size: 452 block weight: 1808 txs: 1 fees: 4520 sigops 408
2017-07-12 04:19:49 UpdateTip: new best=7dd21fe601603d70ecbbec281c730cbc989d494642f1f4fc7597d9e2c0ac507f height=104 version=0x20000000
log2_work=7.7142455 tx=108 date='2017-07-12 04:19:49' progress=1.000000 cache=0.0MiB(4txo)
2017-07-12 04:19:49 AddToWallet 2df639a2d7d160b86311e0d6e16016cf18d905ced7ebab3ea4651a758dc590d6 new
2017-07-12 04:19:49 AddToWallet 09dff07af3819579b4865b9a708643e05d59644890143835a8f019c603dd8afc update
2017-07-12 04:19:49 keypool keep 5

```

B查看余额、区块信息

```

root@localhost:~/bitcoin# /root/bitcoin/src/bitcoin-cli -regtest getbalance
9.99992520
root@localhost:~/bitcoin# /root/bitcoin/src/bitcoin-cli -regtest getinfo
{
  "version": 149900,
  "protocolversion": 70015,
  "walletversion": 139900,
  "balance": 9.99992520,
  "blocks": 104,
  "timeoffset": 0,
  "connections": 0,
  "proxy": "",
  "difficulty": 4.656542373906925e-10,
  "testnet": false,
  "keypoololdest": 1499832144,
  "keypoolsize": 199,
  "paytxfee": 0.00000000,
  "relayfee": 0.00001000,
  "errors": "This is a pre-release test build - use at your own risk - do not use for mining or merchant applications"
}

```

```

B日志
1 147.94.199.129(北京) x 2 172.104.124.159(东京) x +
2017-07-12 04:18:02 init message: Loading P2P addresses...
2017-07-12 04:18:02 Loaded 1 addresses from peers.dat 0ms
2017-07-12 04:18:02 init message: Loading banlist...
2017-07-12 04:18:02 init message: Starting network threads...
2017-07-12 04:18:02 DNS seeding disabled
2017-07-12 04:18:02 init message: Done loading
2017-07-12 04:18:02 msghand thread start
2017-07-12 04:18:02 opencon thread start
2017-07-12 04:18:02 addcon thread start
2017-07-12 04:18:02 net thread start
2017-07-12 04:18:02 Imported mempool transactions from disk: 0 successes, 0 failed, 0 expired
2017-07-12 04:18:02 receive version message: /Satoshi:0.14.99/: version 70015, blocks=103, us=172.104.124.159:28640, peer=0
2017-07-12 04:18:02 Leaving InitialBlockDownload (latching to false)
2017-07-12 04:19:39 Misbehaving: 47.94.199.129:18000 peer=0 (0 -> 100) BAN THRESHOLD EXCEEDED
2017-07-12 04:19:41 receive version message: /Satoshi:0.14.99/: version 70015, blocks=103, us=172.104.124.159:28642, peer=1
2017-07-12 04:19:49 ERROR: ConnectBlock(): CheckInputs on 09dff07af3819579b4865b9a708643e05d59644890143835a8f019c603dd8afc failed with
mandatory-script-verify-flag-failed (Script evaluated without error but finished with a false/empty top stack element) (code 16)
2017-07-12 04:19:49 InvalidChainFound: invalid block=7dd21fe601603d70ecbbec281c730cbc989d494642f1f4fc7597d9e2c0ac507f height=104 log
2_work=7.7142455 date=2017-07-12 04:19:49
2017-07-12 04:19:49 InvalidChainFound: current best=4d4997c23f3d0c8ea547c487762dba72e29d2a64c42bde4d8ed9b15c4b186cdf height=103 log
2_work=7.7004397 date=2017-07-12 04:12:42
2017-07-12 04:19:49 ERROR: ConnectTip(): ConnectBlock 7dd21fe601603d70ecbbec281c730cbc989d494642f1f4fc7597d9e2c0ac507f failed
2017-07-12 04:19:49 InvalidChainFound: invalid block=7dd21fe601603d70ecbbec281c730cbc989d494642f1f4fc7597d9e2c0ac507f height=104 log
2_work=7.7142455 date=2017-07-12 04:19:49
2017-07-12 04:19:49 InvalidChainFound: current best=4d4997c23f3d0c8ea547c487762dba72e29d2a64c42bde4d8ed9b15c4b186cdf height=103 log
2_work=7.7004397 date=2017-07-12 04:12:42

```

图中的服务器 A 的余额 169.99987120，与服务器 B 的余额 20.00000000 验证了新节点服务器 A 向旧节点服务器 B 之间无法转账。表明测试通过。

```

A生成交易地址
1 147.94.199.129(北京) x 2 172.104.124.159(东京) x +
root@i22ze4wxzv9g5i5r69vu05Z:~/bitcoin# /home/sholyn/bitcoin/src/bitcoin-cli -regtest getnewaddress
mjzs9zXGwsR2JX7RCqw2AysL3UBtSNoWri
root@i22ze4wxzv9g5i5r69vu05Z:~/bitcoin#

B给A转10、挖一个区块、查看余额、查看区块信息
1 147.94.199.129(北京) x 2 172.104.124.159(东京) x +
root@localhost:~/bitcoin# /root/bitcoin/src/bitcoin-cli -regtest sendtoaddress mjzs9zXGwsR2JX7RCqw2AysL3UBtSNoWri 10
d142eb91a67c18b2e62087c41899a9c76b6d1644ed06821b350433fd828bd29c
root@localhost:~/bitcoin# /root/bitcoin/src/bitcoin-cli -regtest generate 1
[
  "59f2fbbc0224246e17d39d50c3b024e4b93c127d24c150ec8bc243dbe165dbb3"
]
root@localhost:~/bitcoin# /root/bitcoin/src/bitcoin-cli -regtest getbalance
9.99992520
root@localhost:~/bitcoin# /root/bitcoin/src/bitcoin-cli -regtest getinfo
{
  "version": 149900,
  "protocolversion": 70015,
  "walletversion": 139900,
  "balance": 9.99992520,
  "blocks": 104,
  "timeoffset": 0,
  "connections": 0,
  "proxy": "",
  "difficulty": 4.656542373906925e-10,
  "testnet": false,
  "keypoololdest": 1499832144,
  "keypoolsize": 199,
  "paytxfee": 0.00000000,
  "relayfee": 0.00001000,
  "errors": "This is a pre-release test build - use at your own risk - do not use for mining or merchant applications"
}

```



B日志

```

1 147.94.199.129(北京) x 2 172.104.124.159(东京) x +
2017-07-12 04:25:38 keypool added key 203, size=200, internal=1
2017-07-12 04:25:38 keypool reserve 3
2017-07-12 04:25:38 CreateNewBlock(): total size: 598 block weight: 2392 txs: 1 fees: 7480 sigops 408
2017-07-12 04:25:38 UpdateTip: new best=59f2fbbc0224246e17d39d50c3b024e4b93c127d24c150ec8bc243dbe165dbb3 height=104 version=0x20000000
log2_work=7.7142455 tx=108 date='2017-07-12 04:25:38' progress=1.000000 cache=0.0MiB(6txo)
2017-07-12 04:25:38 AddToWallet 616f6494d60e53bbc18dc55f75258b38976737df319769a231eb2c885d9d0300 new
2017-07-12 04:25:38 AddToWallet d142eb91a67c18b2e62087c41899a9c76b6d1644ed06821b350433fd828bd29c update
2017-07-12 04:25:38 keypool keep 3
2017-07-12 04:26:03 socket recv error Connection reset by peer (104)
2017-07-12 04:27:07 socket recv error Connection reset by peer (104)
2017-07-12 04:27:31 socket recv error Connection reset by peer (104)

```

A日志

```

1 147.94.199.129(北京) x 2 172.104.124.159(东京) x +
CTxOut(nValue=10.00000000, scriptPubKey=76a914914c159a82c698824ab3f3ce)
CTxOut(nValue=19.99987120, scriptPubKey=76a914c9ab7c92cc4647606cbf7676)
2017-07-12 04:19:39 keypool keep 103
2017-07-12 04:19:39 AddToWallet 09dff07af3819579b4865b9a708643e05d59644890143835a8f019c603dd8afc new
2017-07-12 04:19:39 AddToWallet 09dff07af3819579b4865b9a708643e05d59644890143835a8f019c603dd8afc
2017-07-12 04:19:39 Relaying wtx 09dff07af3819579b4865b9a708643e05d59644890143835a8f019c603dd8afc
2017-07-12 04:19:41 receive version message: /Satoshi:0.14.99/: version 70015, blocks=103, us=47.94.199.129:18000, peer=1
2017-07-12 04:19:49 keypool added key 207, size=200, internal=1
2017-07-12 04:19:49 keypool reserve 5
2017-07-12 04:19:49 CreateNewBlock(): total size: 452 block weight: 1808 txs: 1 fees: 4520 sigops 408
2017-07-12 04:19:49 UpdateTip: new best=7dd21fe601603d70ecbbec281c730cbc989d494642f1f4fc7597d9e2c0ac507f height=104 version=0x20000000
log2_work=7.7142455 tx=108 date='2017-07-12 04:19:49' progress=1.000000 cache=0.0MiB(4txo)
2017-07-12 04:19:49 AddToWallet 2df639a2d7d160b86311e0d6e16016cf18d905ced7ebab3ea4651a758dc590d6 new
2017-07-12 04:19:49 AddToWallet 09dff07af3819579b4865b9a708643e05d59644890143835a8f019c603dd8afc update
2017-07-12 04:19:49 keypool keep 5
2017-07-12 04:24:11 keypool added key 208, size=200, internal=0
2017-07-12 04:24:11 keypool reserve 6
2017-07-12 04:24:11 keypool keep 6
2017-07-12 04:25:28 Misbehaving: 172.104.124.159:28642 peer=1 (0 -> 100) BAN THRESHOLD EXCEEDED
2017-07-12 04:25:33 connection from 172.104.124.159:28650 dropped (banned)
2017-07-12 04:25:39 connection from 172.104.124.159:28654 dropped (banned)
2017-07-12 04:25:46 connection from 172.104.124.159:28656 dropped (banned)

```

A查看余额、查看区块信息

```

1 147.94.199.129(北京) x 2 172.104.124.159(东京) x +
root@iZ2ze4wxv9g5iSr69vu05Z:~/.bitcoin# /home/sholyn/bitcoin/src/bitcoin-cli -regtest getbalance
169.99987120
root@iZ2ze4wxv9g5iSr69vu05Z:~/.bitcoin# /home/sholyn/bitcoin/src/bitcoin-cli -regtest getinfo
{
  "version": 149900,
  "protocolversion": 70015,
  "walletversion": 139900,
  "balance": 169.99987120,
  "blocks": 104,
  "timeoffset": 0,
  "connections": 0,
  "proxy": "",
  "difficulty": 4.656542373906925e-10,
  "testnet": false,
  "keypoololdest": 1499832141,
  "keypoolsize": 199,
  "paytxfee": 0.00000000,
  "relayfee": 0.00001000,
  "errors": "This is a pre-release test build - use at your own risk - do not use for mining or merchant applications"
}

```

图中的服务器 A 的余额 169.99987120 ,与服务器 B 的余额 9.99992520 验证了旧节点服务器 B 向新节点服务器 A 无法转账。之间无法转账。表明测试通过。但是此时 A , B 节点区块都是 104 ,但是并不能说明新旧节点区块做了同步。因为此时 A , B 网络中断了。说明 A ,

**B 节点相互已经连不上网络。也从另一个方面可以证明分叉后以后区块链网络也会变成两个网络。**

## 第三章 改进建议

- 方案的设计思想是改变待签的数据内容，使得使用相同的私钥，在新旧两种协议中，产生不同的数字签名。
- 本文方案是对待签名数据内容计算了二次哈希，验证的时候验证的也是待签名内容的二次哈希。

改进方式有两种：

- 为了减小计算量，可以只对待签名数据内容的某个比特取反，验证的时候需要验证的也是对待签名数据内容的某个比特取反后的结果，这种改进方式减小了计算量，但可能带来未知的安全威胁；
- 我们可以直接改变原来的签名中的哈希算法，替换 SHA256 为 SHA3，不仅减小了计算量，也增加了安全性，应该更加合适。