

Regtest en Windows

Instalar el cliente Bitcoin Core.

Vamos a montar 3 nodos, para ello creamos 3 directorios de datos en la ruta que queramos, en mi caso en c:\regtest

Disco local (C:) > regtest >				
	Nombre	Fecha de modifica...	Tipo	Tamaño
★	node1	24/09/2018 8:27	Carpeta de archivos	
★	node2	24/09/2018 8:28	Carpeta de archivos	
★	node3	24/09/2018 8:28	Carpeta de archivos	

Generamos dentro de cada carpeta un bitcoin.conf con el usuario y pass de rpc, para pruebas ponemos usuario y pass con el nombre del nodo:

```
bitcoin.conf: Bloc de notas
Archivo Edición Formato Ver Ayuda
# [rpc]
# Username for JSON-RPC connections
rpcuser=node1
# Password for JSON-RPC connections
rpcpassword=node1
```

Iniciamos cada nodo con su comando:

```
bitcoind -regtest -port=8333 -rpcport=8332 -datadir=c:\regtest\node1 -conf=c:\regtest\node1\bitcoin.conf
bitcoind -regtest -port=8335 -rpcport=8334 -datadir=c:\regtest\node2 -conf=c:\regtest\node2\bitcoin.conf
bitcoind -regtest -port=8337 -rpcport=8336 -datadir=c:\regtest\node3 -conf=c:\regtest\node3\bitcoin.conf
```

Generamos bloques (101 bloques)

```
bitcoin-cli -regtest -rpcuser=node1 -rpcpassword=node1 -rpcport=8332 -rpcport=8332 generate 101
```

Comprobamos saldo

```
bitcoin-cli -regtest -rpcuser=node1 -rpcpassword=node1 -rpcport=8332 -rpcport=8332 getbalance
```

En la información del nodo1 vemos que no tiene peers

```
bitcoin-cli -regtest -rpcuser=node1 -rpcpassword=node1 -rpcport=8332 -rpcport=8332 --getinfo
```

```
C:\Program Files\Bitcoin\daemon>bitcoin-cli -regtest -rpcuser=node1 -rpcpassword=node1 -rpcport=8332 -rpcport=8332 --getinfo
{
  "version": 160300,
  "protocolversion": 70015,
  "walletversion": 159900,
  "balance": 50.00000000,
  "blocks": 101,
  "timeoffset": 0,
  "connections": 0,
  "proxy": "",
  "difficulty": 4.656542373906925e-010,
  "testnet": false,
  "keypoololdest": 1537772013,
  "keypoolsize": 999,
  "paytxfee": 0.00000000,
  "relayfee": 0.00001000,
  "warnings": ""
}
```

Lo conectamos a los otros 2 nodos.

```
bitcoin-cli -regtest -rpcport=8332 -rpcuser=node1 -rpcpassword=node1 addnode 127.0.0.1:8335 add
```

```
bitcoin-cli -regtest -rpcport=8332 -rpcuser=node1 -rpcpassword=node1 addnode 127.0.0.1:8337 add
```

Comprobamos que tiene 2 conexiones

```
bitcoin-cli -regtest -rpcuser=node1 -rpcpassword=node1 -rpcport=8332 getconnectioncount
```

```
C:\Program Files\Bitcoin\daemon>bitcoin-cli -regtest -rpcuser=node1 -rpcpassword=node1 -rpcport=8332 getconnectioncount
2
```

Si comprobamos el nodo 2 y 3 deberían tener 1 conexión y ver los 101 bloques que hemos generado en el nodo 1.

```
bitcoin-cli -regtest -rpcuser=node2 -rpcpassword=node2 -rpcport=8334 --getinfo
```

```
C:\Program Files\Bitcoin\daemon>bitcoin-cli -regtest -rpcuser=node2 -rpcpassword=node2 -rpcport=8334 --getinfo
{
  "version": 160300,
  "protocolversion": 70015,
  "walletversion": 159900,
  "balance": 0.00000000,
  "blocks": 101,
  "timeoffset": 0,
  "connections": 1,
  "proxy": "",
  "difficulty": 4.656542373906925e-010,
  "testnet": false,
  "keypoololdest": 1537772024,
  "keypoolsize": 1000,
  "paytxfee": 0.00000000,
  "relayfee": 0.00001000,
  "warnings": ""
}

C:\Program Files\Bitcoin\daemon>bitcoin-cli -regtest -rpcuser=node3 -rpcpassword=node3 -rpcport=8336 --getinfo
{
  "version": 160300,
  "protocolversion": 70015,
  "walletversion": 159900,
  "balance": 0.00000000,
  "blocks": 101,
  "timeoffset": 0,
  "connections": 1,
  "proxy": "",
  "difficulty": 4.656542373906925e-010,
  "testnet": false,
  "keypoololdest": 1537772029,
  "keypoolsize": 1000,
  "paytxfee": 0.00000000,
  "relayfee": 0.00001000,
  "warnings": ""
}
```

Vamos a realizar una transacción para comprobar que se propaga. Para ello creamos una nueva dirección en el nodo 2

```
bitcoin-cli -regtest -rpcuser=node2 -rpcpassword=node2 -rpcport=8334 getnewaddress
```

```
C:\Program Files\Bitcoin\daemon>bitcoin-cli -regtest -rpcuser=node2 -rpcpassword=node2 -rpcport=8334 getnewaddress
2N6FEkFMsx8MpGwAAmyyg6yeaDjQ8nPH6XS
```

Y enviamos 1BTC desde nuestro nodo 1.

```
bitcoin-cli -regtest -rpcuser=node1 -rpcpassword=node1 -rpcport=8332 sendtoaddress
```

```
2N6FEkFMsx8MpGwAAmyyg6yeaDjQ8nPH6XS 1
```

```
C:\Program Files\Bitcoin\daemon>bitcoin-cli -regtest -rpcuser=node1 -rpcpassword=node1 -rpcport=8332 sendtoaddress 2N6FEkFMsx8MpGwAAmyyg6yeaDjQ8nPH6XS 1
60b46a9f9972b7829308e7de9617c91c42518db994a1497d41e7c4527148f448
```

Con esto hemos generado la transacción

```
60b46a9f9972b7829308e7de9617c91c42518db994a1497d41e7c4527148f448
```

Comprobamos que en la mempool de los nodos existe esta transacción con el comando:

```
bitcoin-cli -regtest -rpcuser=node1 -rpcpassword=node1 -rpcport=8332 getrawmempool
```

```
C:\Program Files\Bitcoin\daemon>bitcoin-cli -regtest -rpcuser=node2 -rpcpassword=node2 -rpcport=8334 getrawmempool
[
  "60b46a9f9972b7829308e7de9617c91c42518db994a1497d41e7c4527148f448"
]

C:\Program Files\Bitcoin\daemon>bitcoin-cli -regtest -rpcuser=node3 -rpcpassword=node3 -rpcport=8336 getrawmempool
[
  "60b46a9f9972b7829308e7de9617c91c42518db994a1497d41e7c4527148f448"
]

C:\Program Files\Bitcoin\daemon>bitcoin-cli -regtest -rpcuser=node1 -rpcpassword=node1 -rpcport=8332 getrawmempool
[
  "60b46a9f9972b7829308e7de9617c91c42518db994a1497d41e7c4527148f448"
]
```

Bien, tenemos la transacción en la mempool de los 3 nodos. Vamos a generar 1 bloque para confirmarla.

Antes comprobamos que está sin confirmar en el nodo 2 (al que hemos enviado la tx)

```
bitcoin-cli -regtest -rpcuser=node2 -rpcpassword=node2 -rpcport=8334 getunconfirmedbalance
```

```
C:\Program Files\Bitcoin\daemon>bitcoin-cli -regtest -rpcuser=node2 -rpcpassword=node2 -rpcport=8334 getunconfirmedbalance
1.00000000
```

Minamos 1 bloque desde el nodo1 con

```
bitcoin-cli -regtest -rpcuser=node1 -rpcpassword=node1 -rpcport=8332 generate 1
```

```
C:\Program Files\Bitcoin\daemon>bitcoin-cli -regtest -rpcuser=node1 -rpcpassword=node1 -rpcport=8332 generate 1
[
  "49ee0496da7eff06addcbcb9d1183a3151caed51586987b6b00bafce96ee11"
]
```

Comprobamos que el bitcoin enviado ha pasado de estar sin confirmar a estar confirmado y la tx ha desaparecido de las mempool:

```
C:\Program Files\Bitcoin\daemon>bitcoin-cli -regtest -rpcuser=node2 -rpcpassword=node2 -rpcport=8334 getunconfirmedbalance
0.00000000

C:\Program Files\Bitcoin\daemon>bitcoin-cli -regtest -rpcuser=node2 -rpcpassword=node2 -rpcport=8334 getbalance
1.00000000

C:\Program Files\Bitcoin\daemon>bitcoin-cli -regtest -rpcuser=node1 -rpcpassword=node1 -rpcport=8332 getrawmempool
[
]

C:\Program Files\Bitcoin\daemon>bitcoin-cli -regtest -rpcuser=node2 -rpcpassword=node2 -rpcport=8334 getrawmempool
[
]

C:\Program Files\Bitcoin\daemon>bitcoin-cli -regtest -rpcuser=node3 -rpcpassword=node3 -rpcport=8336 getrawmempool
[
]
```

Vamos a crear una transacción sin la opción de RBF (Replace By Fee) para ello comenzamos creando una nueva address en el nodo 3 con:

```
bitcoin-cli -regtest -rpcuser=node3 -rpcpassword=node3 -rpcport=8336 getnewaddress
```

Nos devuelve nuestra nueva dirección:

```
2Myq4pynBLLVi5wfj7ngEEedSm1H3YY8CfMv
```

```
bitcoin-cli -regtest -rpcuser=node1 -rpcpassword=node1 -rpcport=8332 listunspent
```

Vemos que tenemos 2 UTXO que podemos utilizar para crear la transacción, vamos a mandar 1BTC a la dirección del nodo 3 que hemos creado hace un rato. El formato para crear transacciones es el siguiente:

```
{["txid": "<txid_of_selected_block>",
  "vout": <vout>
}]
{"<recipient address>": <amount to send>, "<sender address>": <amount change>}
```

"{"2Myq4pynBLLVi5wfi7ngEEedSm1H3YY8CfMv\":1,\"2NDBW6T9y8nr9Xivd6hPRdiEM8jpGtnXPnu\":47.99995616}"

Y nos devolverá otra cadena con nuestra transacción firmada, en este caso:

[illegible]

```
C:\Program Files\Bitcoin\daemon>bitcoin-cli -regtest -rpcuser=node1 -rpcpassword=node1 -rpcport=8332 getrawmempool
["d9a7deb4c087d90423d99b78dc2f31e5b6f8e24fc0a194fc49db97e93f60c09b"]

C:\Program Files\Bitcoin\daemon>bitcoin-cli -regtest -rpcuser=node2 -rpcpassword=node2 -rpcport=8334 getrawmempool
["d9a7deb4c087d90423d99b78dc2f31e5b6f8e24fc0a194fc49db97e93f60c09b"]

C:\Program Files\Bitcoin\daemon>bitcoin-cli -regtest -rpcuser=node3 -rpcpassword=node3 -rpcport=8336 getrawmempool
["d9a7deb4c087d90423d99b78dc2f31e5b6f8e24fc0a194fc49db97e93f60c09b"]
```

La firmamos y la enviamos, no nos permite hacerlo por existir en la mempool:


```
bitcoin-cli -regtest -rpcuser=node1 -rpcpassword=node1 -rpcport=8332 signrawtransaction
0200000000123b825138875dcd2fcea5a6e7b0bbcb550e92f2755f37745c59b086871af5e4a0100000000fdffffff0200e1f505000000
0017a9143c1b077216feaad3627c23a3670144f7ae79303f87684d2e120100000017a914daae4bf62e879ba69935f1f1a9aa770af
3e599cb8700000000
```

La enviamos:

```
bitcoin-cli -regtest -rpcuser=node1 -rpcpassword=node1 -rpcport=8332 sendrawtransaction
0200000000010123b825138875dcd2fcea5a6e7b0bbcb550e92f2755f37745c59b086871af5e4a0100000017160014235a8e2a3
5fd9db351160372cb964614db2d40d9fdffffff0200e1f5050000000017a9143c1b077216feaad3627c23a3670144f7ae79303f87684
d2e120100000017a914daae4bf62e879ba69935f1f1a9aa770af3e599cb87024730440220023669a6f7a944d501a9286e3330f88
8df6b205725afb28e55d35874a3b6f5390220242252b40b28a62351344093e9d7f2b2626c58025696439fd89c41bea9c2822c012
102dcc6343071498b3766a6100d9e623b4c9ae5af0de8125e83450734f622f380bc00000000
7d808fd7b6982f2a11349c2ac63aa51477357e0b2c90145498decddbea20208d
```

Nos devuelve el txid 7d808fd7b6982f2a11349c2ac63aa51477357e0b2c90145498decddbea20208d

Comprobamos que está en la mempool de todos los nodos:

```
C:\Program Files\Bitcoin\daemon>bitcoin-cli -regtest -rpcuser=node1 -rpcpassword=node1 -rpcport=8332 getrawmempool
[
  "7d808fd7b6982f2a11349c2ac63aa51477357e0b2c90145498decddbea20208d"
]

C:\Program Files\Bitcoin\daemon>bitcoin-cli -regtest -rpcuser=node2 -rpcpassword=node2 -rpcport=8334 getrawmempool
[
  "7d808fd7b6982f2a11349c2ac63aa51477357e0b2c90145498decddbea20208d"
]

C:\Program Files\Bitcoin\daemon>bitcoin-cli -regtest -rpcuser=node3 -rpcpassword=node3 -rpcport=8336 getrawmempool
[
  "7d808fd7b6982f2a11349c2ac63aa51477357e0b2c90145498decddbea20208d"
]
```

Generamos la transacción subiendo la comisión y la dirección de destino:

```
bitcoin-cli -regtest -rpcuser=node1 -rpcpassword=node1 -rpcport=8332 createrawtransaction "[{"txid":
\"4a5eaf7168089bc54577f355272fe950b5bc0b7b6e5aeafcd2dc75881325b823\", \"vout\": 1}]"
{"2N6FEkFMsx8MpGwAAmyy6yeadJQ8nPH6XS":1,\"2NBDW6T9y8nr9Xivd6hPRdiEM8jpGtnXPnu\":45.99991356}" 0 true
```

La firmamos y la enviamos.

En el log (debug.log)

```
2018-09-24 08:39:28 Potential stale tip detected, will try using extra outbound peer (last tip update: 3886 seconds ago)
2018-09-24 08:40:42 UpdateTip: new best=364bdfefef19ceb0b1af1895f68097d32c24014aa12a7150c66885693b2228 height=103 version=0x20000000 log2_work=7.7004397 tx=106 date='2018-09-24 08:40:42' progress=1.000000 cache=0.0M...
2018-09-24 09:10:58 Potential stale tip detected, will try using extra outbound peer (last tip update: 1816 seconds ago)
2018-09-24 09:21:28 Potential stale tip detected, will try using extra outbound peer (last tip update: 2446 seconds ago)
2018-09-24 09:25:29 UpdateTip: new best=4c7f6b97aede4402e71d4e0250b63dd980236c0ee8a699942958056f520ee859 height=104 version=0x20000000 log2_work=7.7142455 tx=108 date='2018-09-24 09:25:29' progress=1.000000 cache=0.0...
2018-09-24 09:41:20 AddToWallet 7d808fd7b6982f2a11349c2ac63aa51477357e0b2c90145498decddbea20208d new
2018-09-24 09:54:07 AddToWallet 649d0035c6d829d5e3fb3aaf297847dfca7bd4fbb6e26e319c87d06714ee677d new
```

Vemos como añade la primera y la segunda.

Comprobamos la mempool de los 3 nodos y vemos que sólo existe la segunda transacción:

```
C:\Program Files\Bitcoin\daemon>bitcoin-cli -regtest -rpcuser=node1 -rpcpassword=node1 -rpcport=8332 getrawmempool
[
  "649d0035c6d829d5e3fb3aaf297847dfca7bd4fbb6e26e319c87d06714ee677d"
]

C:\Program Files\Bitcoin\daemon>bitcoin-cli -regtest -rpcuser=node2 -rpcpassword=node2 -rpcport=8334 getrawmempool
[
  "649d0035c6d829d5e3fb3aaf297847dfca7bd4fbb6e26e319c87d06714ee677d"
]

C:\Program Files\Bitcoin\daemon>bitcoin-cli -regtest -rpcuser=node3 -rpcpassword=node3 -rpcport=8336 getrawmempool
[
  "649d0035c6d829d5e3fb3aaf297847dfca7bd4fbb6e26e319c87d06714ee677d"
]
```

Con RBF puedes modificar la dirección de destino.