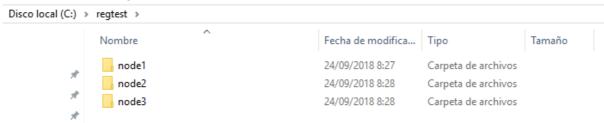
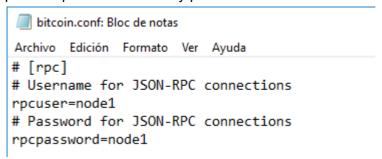
Regtest en Windows Instalar el cliente Bitcoin Core.

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



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:



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": 50.0000000,
    "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,
    "keypoolsize": 1000,
    "paytxfee": 0.0000000,
    "relayfee": 0.0000000,
    "relayfee": 0.00000100,
    "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,
    "keypooloidest": 1537777029,
    "keypoolsize": 1000,
    "paytxfee": 0.00000000,
    "relayfee": 0.00000000,
    "relayfee": 0.00000000,
    "paytxfee": 0.00000000,
    "relayfee": 0.00000000,
    "relayf
```

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 envíamos 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=nodel -rpcpassword=nodel -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 envíado 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
```

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
[
"49ee0496da7eff06addcbcbb9d1183a3151caed51586987b6b00bafece96ee11"
]
```

Comprobamos que el bitcoin envíado 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=node2 -rpcpassword=node2 -rpcport=8336 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:

2Myq4pynBLLVi5wfj7ngEEdSm1H3YY8CfMv

Creamos una transacción desde el nodo 1, para ello tenemos que saber los UTXO que tenemos disponibles:

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:

Así que nuestra transacción sería así:

```
bitcoin-cli -regtest -rpcuser=node1 -rpcpassword=node1 -rpcport=8332 createrawtransaction "[{\"txid\":\"60b46a9f9972b7829308e7de9617c91c42518db994a1497d41e7c4527148f448\",\"vout\": 0}]" "{\"2Myq4pynBLLVi5wfj7ngEEdSm1H3YY8CfMv\":1,\"2NDBW6T9y8nr9Xivd6hPRdiEM8jpGtnXPnu\":47.99995616}"
```

Nos devolverá una cadena hexadecimal que contiene el detalle de nuestra transacción. En este caso:

 $020000000148f4487152c4e7417d49a194b98d51421cc91796dee7089382b772999f6ab46000000000000fffffff0200e1f50500000\\00017a9144837402c11ab359d3622aaf868486b24b5d53dd987e01e1a1e0100000017a914daae4bf62e879ba69935f1f1a9aa77\\0af3e599cb870000000$

Firmamos nuestra transacción con:

bitcoin-cli -regtest -rpcuser=node1 -rpcpassword=node1 -rpcport=8332 signrawtransaction 020000000148f4487152c4e7417d49a194b98d51421cc91796dee7089382b772999f6ab46000000000000fffffff0200e1f50500000 00017a9144837402c11ab359d3622aaf868486b24b5d53dd987e01e1a1e0100000017a914daae4bf62e879ba69935f1f1a9aa77 0af3e599cb870000000

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

020000000010148f4487152c4e7417d49a194b98d51421cc91796dee7089382b772999f6ab460000000017160014235a8e2a 35dfddb351160372cb964614db2d40d9fffffff0200e1f5050000000017a9144837402c11ab359d3622aaf868486b24b5d53dd987e 01e1a1e0100000017a914daae4bf62e879ba69935f1f1a9aa770af3e599cb870248304502210088dfda379492eb0c5b2b2240177 598c8e7791902da23f90f1e25e1bfae4257360220171611fd07dae7482d2e7eb27f6a62bec6780e52f269115f080392f55434f5760 12102dcc6343071498b3766a6100d9e623b4c9ae5af0de8125e83450734f622f380bc00000000

Propagamos nuestra transacción con

bitcoin-cli -regtest -rpcuser=node1 -rpcpassword=node1 -rpcport=8332 sendrawtransaction
020000000010148f4487152c4e7417d49a194b98d51421cc91796dee7089382b772999f6ab460000000017160014235a8e2a
35dfddb351160372cb964614db2d40d9fffffff0200e1f5050000000017a9144837402c11ab359d3622aaf868486b24b5d53dd987e
01e1a1e0100000017a914daae4bf62e879ba69935f1f1a9aa770af3e599cb870248304502210088dfda379492eb0c5b2b2240177
598c8e7791902da23f90f1e25e1bfae4257360220171611fd07dae7482d2e7eb27f6a62bec6780e52f269115f080392f55434f5760
12102dcc6343071498b3766a6100d9e623b4c9ae5af0de8125e83450734f622f380bc00000000
d9a7deb4c087d90423d99b78dc2f31e5b6f8e24fc0a194fc49db97e93f60c09b

Comprobamos que la transacción está en todos las mempool con

bitcoin-cli -regtest -rpcuser=node1 -rpcpassword=node1 -rpcport=8332 getrawmempool bitcoin-cli -regtest -rpcuser=node2 -rpcpassword=node2 -rpcport=8334 getrawmempool bitcoin-cli -regtest -rpcuser=node3 -rpcpassword=node3 -rpcport=8336 getrawmempool

```
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"

"d9a7deb4c087d90423d99b78dc2f31e5b6f8e24fc0a194fc49db97e93f60c09b"
```

Generamos una dirección en el nodo 2 con

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

Nos devuelve nuestra nueva dirección:

2Mxj2uongmNmJui2UrUeJSDPa97PuwsdvaX

Generamos la transacción utilizando el mismo UTXO y modificando la dirección de destino:

 $\label{lem:licoin-cli-regtest-recuser-node1-reconstance} bitcoin-cli-regtest-recuser-node1-reconstance 1-reconstance 1-reconst$

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

```
C:\Program Files\Bitcoin\daemon>bitcoin-cli -regtest -rpcuser=node1 -rpcpassword
7de9617c91c42518db994a1497d41e7c4527148f448\",\"vout\": 0}]" "{\"2Mxj2uongmNmJui
7de9617c91c42518db994a1497d41e7c4527148f448\",\"vout\": 0}]" "{\"2Mxj2uongmNmJui
7de9617c91c42518db994a1497d41e7c4527148f448\",\"vout\": 0}]" "{\"2Mxj2uongmNmJui
7de9617c91c42518db994a1497d41e7c4527148f448\",\"vout\": 0}]" "{\"2Mxj2uongmNmJui
7de96121c291796dee708934674999f6ab4690935f1f1a9aa770af3e599cb870000000
C:\Program Files\Bitcoin\daemon>bitcoin-cli -regtest -rpcuser=node1 -rpcpassword
651421cc91796dee7089382b772999f6ab46000000000ffffffffff0200e1f50500000000017a9143
669935f1f1a9aa770af3e599cb870000000
{
    "hex": "020000000010148f4487152c4e7417d49a194b98d51421cc91796dee7089382b77299
1f5050000000017a9143c1b077216feaad3627c23a3670144f7ae79303f87e01e1a1e0100000017a
62641ba8da16bc9fe22155a16b6736d59e71e50ffd9387c02207c92f13f7c9da1ce93093f8d083370
f0de8125e83450734f622f380bc000000000",
    "complete": true
}
C:\Program Files\Bitcoin\daemon>bitcoin-cli -regtest -rpcuser=node1 -rpcpassword
4b98d51421cc91796dee7089382b772999f6ab460000000017160014235a8e2a35dfddb35116037
44f7ae79303f87e01e1a1e0100000017a914daae4bf62e879ba69935f1f1a9aa770af3e599cb8702
2207c92f13f7c9da1ce93093f8d083370316274b899778872bc3c21f63a1bcad671012102dcc6343
error code: -26
error message:
18: txn-mempool-conflict
```

Minamos un bloque para confirmar la primera transacción y despejar la mempool

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

"364bdfeeef19cebd0b1af1895f68097d32c24014aa12a7150c668885693b2228"

C:\Program Files\Bitcoin\daemon>
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=node2 -rpcpassword=node2 -rpcport=8334 getrawmempool

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

Repetimos el proceso con RBF, para generar una transacción con RBF sólo tenemos que añadir el campo true al final del comando createrawtransaction, comprobamos los UTXO disponibles con

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

Generamos la transacción con RBF:

 $bitcoin-cli-regtest-rpcuser=node1-rpcpassword=node1-rpcport=8332\ createrawtransaction\ "[{\"txid\": \''4a5eaf7168089bc54577f355272fe950b5bc0b7b6e5aeafcd2dc75881325b823\", \"vout\": 1}]" \\ "{\"2Mxj2uongmNmJui2UrUeJSDPa97PuwsdvaX\":1,\"2NDBW6T9y8nr9Xivd6hPRdiEM8jpGtnXPnu\":45.99991656}"\ 0\ true$

La firmamos:

bitcoin-cli -regtest -rpcuser=node1 -rpcpassword=node1 -rpcport=8332 signrawtransaction 020000000123b825138875dcd2fcea5a6e7b0bbcb550e92f2755f37745c59b086871af5e4a0100000000fdfffff0200e1f505000000 0017a9143c1b077216feaad3627c23a3670144f7ae79303f87684d2e120100000017a914daae4bf62e879ba69935f1f1a9aa770af 3e599cb870000000

La enviamos:

bitcoin-cli -regtest -rpcuser=node1 -rpcpassword=node1 -rpcport=8332 sendrawtransaction
020000000010123b825138875dcd2fcea5a6e7b0bbcb550e92f2755f37745c59b086871af5e4a0100000017160014235a8e2a3
5dfddb351160372cb964614db2d40d9fdfffff0200e1f5050000000017a9143c1b077216feaad3627c23a3670144f7ae79303f87684
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=nodel -rpcpassword=nodel -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:

 $\label{lem:bitcoin-cli-regtest-recuser-node1-reconstance} bitcoin-cli-regtest-recuser-node1-reconstance-reconsta$

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 Update Fip: new best=364bdfeeef19cebd0b1af1895f68097d32c24014sa12a7150c66885693b2228 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=47f6b97aede4402e71d4e0250b63dd980236-0ee8a699942958056f520ee859 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 09:54:07 AddToWallet 7d808fd7b698272a11349C2ac63as31477357e0b2c90145498decddbea202008d new
2018-09-24 09:54:07 AddToWallet 649d0035c6d82945e3fb3asf297847dfca7bd4fbb6e26c319c87d00714ee677d 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=nodel -rpcpassword=nodel -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.