

## Blockchain & Cryptocurrency Lab 2

Batman's address (mgz7sshZaZ57A9tUmMs1yAc2ZdesBATMAN)

Robin's address (mio1EsCc7tfHNZqqxDC4x826UTAE6RoBiN)

1. First we need some coins to be able to send to Batman and Commissioner Gordon. Used the faucet website from Lab 1 <https://bitcoinafaucet.uo1.net/send.php> and <https://coinafaucet.eu/en/btc-testnet/> to get coins

Bitcoin testnet3 faucet

Donate?

We sent **0.0376542** bitcoins to address  
tb1qxlazmn8lg7z8e9548e6xqtkfwsgxj7a325u73  
tx: 002e0f169519ca4619f7c673b32788c8f636ab8a1b03166482c2a65e20da43aa  
Send coins back, when you don't need them anymore to the address  
mv4rnyY3Su5gjcDNzbMLKBQkBicCtHUtFB

Back

Bitcoin Talk Thread

0.00005282 coins sent to tb1qxlazmn8lg7z8e9548e6xqtkfwsgxj7a325u73. Don't forget to send the testnet coins back when you're done with them

₿


tb1qxlazmn8lg7z8e9548e6xqtkfwsgxj7a325u73

0.00001

Send testnet bitcoins

BTC Address

Send testnet coins back, when you don't need them anymore: [tb1q4280xax2lt0u5a5s9hd4easuvzalm8v9ege9ge](#)



Last Transactions

2. Next get the UTXOs for input using this command

```
22:13:48 2 listunspent
22:13:48 2 {
  {
    "txid": "c80367b1a7f6ea8831abeea3c584aef19361c76cb0f603865a11dc2aaa467042",
    "vout": 1,
    "address": "tb1qxlazmn8lg7z8e9548e6xqtkfwsgxj7a325u73",
    "label": "",
    "scriptPubKey": "001437fa416e67fa3c23e4b4a9f3a301764ba0834bdd",
    "amount": 0.03705420,
    "confirmations": 1,
    "spendable": true,
    "solvable": true,
    "desc": "wpkh([da5e8515/0'/0'/3']03c596f98eda8ce9774b28545ac250279e1b59ecc6e4adee330d0eea386c42d4d1)#95klxze3",
    "safe": true
  }
}
```

3. Next we get the public key address information using this command, to verify my address ownership

```
22:15:09 getaddressinfo "tblqxlayzmn8lg7z8e9548e6xqtkfwsgxj7a325u73"
22:15:09 {
  "address": "tblqxlayzmn8lg7z8e9548e6xqtkfwsgxj7a325u73",
  "scriptPubKey": "001437fa416e67fa3c23e4b4a9f3a301764ba0834bdd",
  "ismine": true,
  "solvable": true,
  "desc": "wpkh([da5e8515/0'/0'/3']03c596f98eda8ce9774b28545ac250279e1b59ecc6e4adee330d0eea386c42d4d1)#95k1xe3",
  "iswatchonly": false,
  "isscript": false,
  "iswitness": true,
  "witness_version": 0,
  "witness_program": "37fa416e67fa3c23e4b4a9f3a301764ba0834bdd",
  "pubkey": "03c596f98eda8ce9774b28545ac250279e1b59ecc6e4adee330d0eea386c42d4d1",
  "ischange": false,
  "timestamp": 1678612947,
  "hdkeypath": "m/0'/0'/3'",
  "hdseedid": "0c9bf720e10b166a48b7e1d28b12719386ec09b6",
  "hdmasterfingerprint": "da5e8515",
  "labels": [
    ""
  ]
}
```

4. Now we need to create raw transactions for Batman and Robin

```
22:17:59 createrawtransaction [{"txid": "c80367b1a7f6ea8831abeea3c584aef19361c76cb0f603865a11dc2aaa467042", "vout": 1}] [{"mgz7ssh2a257A9tUmM5lyAc22desBATMAN": 0.03705420}] 0 true
22:17:59 0200000001427046aa2adc115a8603f6b06cc76193f1ae84c5a3eeab3188eafea7b16703c80100000000fdffffff014c8a3800000000001976a914101b5b38eb3bd658689e7098f02709f3ada9da3a88ac00000000
22:18:16 createrawtransaction [{"txid": "c80367b1a7f6ea8831abeea3c584aef19361c76cb0f603865a11dc2aaa467042", "vout": 1}] [{"mio1EsCc7tfHNZqxD4x826UTAE6RoB1N": 0.03705420}] 0 true
22:18:16 0200000001427046aa2adc115a8603f6b06cc76193f1ae84c5a3eeab3188eafea7b16703c80100000000fdffffff014c8a3800000000001976a91423f17dbb0dde49ef3af1a2112eb9b60215ec203d88ac00000000
```

5. Then I funded the raw transactions for Batman and Robin

```
22:18:54 fundrawtransaction
"0200000001427046aa2adc115a8603f6b06cc76193f1ae84c5a3eeab3188eafea7b16703c80100000000fdffffff014c8a3800000000001976a914101b5b38eb3bd658689e7098f02709f3ada9da3a88ac00000000" [{"changeAddress": "tblqxlayzmn8lg7z8e9548e6xqtkfwsgxj7a325u73", "includeWatching": false, "feeRate": 0.00005, "replaceable": true, "changePosition": 1, "subtractFeeFromOutputs": [0]}] true
22:18:54 {
  "hex":
    "0200000001427046aa2adc115a8603f6b06cc76193f1ae84c5a3eeab3188eafea7b16703c80100000000fdffffff0117883800000000001976a914101b5b38eb3bd658689e7098f02709f3ada9da3a88ac00000000",
  "fee": 0.00000565,
  "changePos": -1
}
22:19:21 fundrawtransaction
"0200000001427046aa2adc115a8603f6b06cc76193f1ae84c5a3eeab3188eafea7b16703c80100000000fdffffff014c8a3800000000001976a91423f17dbb0dde49ef3af1a2112eb9b60215ec203d88ac00000000" [{"changeAddress": "tblqxlayzmn8lg7z8e9548e6xqtkfwsgxj7a325u73", "includeWatching": false, "feeRate": 0.00005, "replaceable": true, "changePosition": 1, "subtractFeeFromOutputs": [0]}] true
22:19:21 {
  "hex":
    "0200000001427046aa2adc115a8603f6b06cc76193f1ae84c5a3eeab3188eafea7b16703c80100000000fdffffff0117883800000000001976a91423f17dbb0dde49ef3af1a2112eb9b60215ec203d88ac00000000",
  "fee": 0.00000565,
  "changePos": -1
}
```

6. After verifying with my wallet passphrase, I signed both raw transactions for Batman and Robin

```
22:19:47 walletpassphrase(...)
22:19:47 null
22:20:19 signrawtransactionwithwallet
"0200000001427046aa2adc115a8603f6b06cc76193f1ae84c5a3eeab3188eafea7b16703c80100000000fdffffff0117883800000000001976a914101b5b38eb3bd658689e7098f02709f3ada9da3a88ac00000000" [{"txid": "c80367b1a7f6ea8831abeea3c584aef19361c76cb0f603865a11dc2aaa467042", "vout": 0, "scriptPubKey": "001437fa416e67fa3c23e4b4a9f3a301764ba0834bdd", "amount": 0.03705420}]
22:20:19 {
  "hex":
    "02000000000101427046aa2adc115a8603f6b06cc76193f1ae84c5a3eeab3188eafea7b16703c80100000000fdffffff0117883800000000001976a914101b5b38eb3bd658689e7098f02709f3ada9da3a88ac0247304402206502735e36f669b1289b5db0889264fa0c67faf2c72d50314f8fa283ebb066002205872de39b7303628dd9d9b5f05f4e7dada33f9d98cf532ace18e2c90b7a df22e012103c596f98eda8ce9774b28545ac250279e1b59ecc6e4adee330d0eea386c42d4d100000000",
  "complete": true
}
22:20:40 signrawtransactionwithwallet
"ec203d88ac00000000" [{"txid": "c80367b1a7f6ea8831abeea3c584aef19361c76cb0f603865a11dc2aaa467042", "vout": 0, "scriptPubKey": "001437fa416e67fa3c23e4b4a9f3a301764ba0834bdd", "amount": 0.03705420}]
22:20:40 {
  "hex":
    "02000000000101427046aa2adc115a8603f6b06cc76193f1ae84c5a3eeab3188eafea7b16703c80100000000fdffffff0117883800000000001976a91423f17dbb0dde49ef3af1a2112eb9b60215ec203d88ac0247304402204f97c2a2be2c02064daef370afe7494ba3416c6b9b3e3feed56cf4fecbcd2102201c6513ab2942ed542b99518de8c5ed256bea6e03378da0c97530d45b294 46c5a012103c596f98eda8ce9774b28545ac250279e1b59ecc6e4adee330d0eea386c42d4d100000000",
  "complete": true
}
```

## 7. I verified my transactions with testmempoolaccept before broadcasting

```
22:21:20 testmempoolaccept
'["02000000000101427046aa2adc115a8603f6b06cc76193f1ae84c5a3eeab3188eafea7b16703c80100000000fdffffff0117883800000000001976a914101b5b38eb3bd658689e7098f02709f3ada9da3a88ac02473044022066502735e36f669b1289b5db0889264fa0c67fa2c72d50314f8fa283ebb066002205872de39b7303628dd9d9b5f05f4e7dada33f9d98cf532ace18e2c90b7adf22e012103c596f98eda8ce9774b28545ac250279e1b59ecc6e4adee330d0eea386c42d4d100000000"]]'

22:21:20 {
  "txid": "25f05bdebb792dfb45c060e64d44cdb6faaca3a68ec99be742646fe5bf311549",
  "wtxid": "898bc2ac0cf178e927509bcbcc5400e243f647a555b6d720bcc483e6e1046644e",
  "allowed": true,
  "vsize": 113,
  "fees": {
    "base": 0.00000565
  }
}

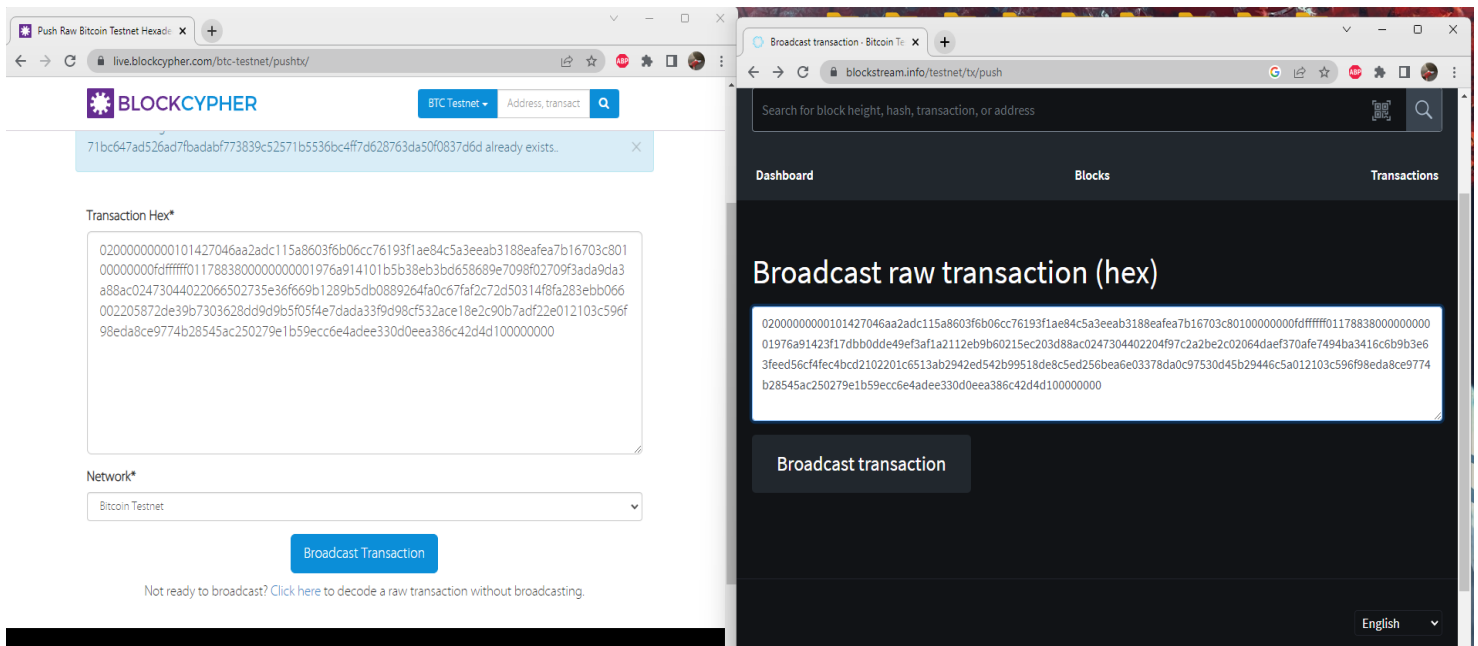
22:21:53 testmempoolaccept
'["02000000000101427046aa2adc115a8603f6b06cc76193f1ae84c5a3eeab3188eafea7b16703c80100000000fdffffff0117883800000000001976a91423f17dbb0dde49ef3af1a2112eb9b60215ac203d88ac0247304402204f97c2a2be2c02064dae370afe7494ba3416c6b9b3e63feed56cf4fec4bcd2102201c6513ab2942ed542b99518de8c5ed256bea6e03378da0c97530d45b29446c5a012103c596f98eda8ce9774b28545ac250279e1b59ecc6e4adee330d0eea386c42d4d100000000"]]'

22:21:53 {
  "txid": "ef46554e8b76d79df3f47b712d4236f9391cd9840bc13ba7ed0150d1993ede0",
  "wtxid": "fc09dbf580cd23408c5798663d085e9ae9de27286a98f1391e356724b0f9824b",
  "allowed": true,
  "vsize": 113,
  "fees": {
    "base": 0.00000565
  }
}
```


## 8. Now we need to send both raw transactions simultaneously. For both I used an online service to broadcast the transaction with the following websites,


Batman: <https://live.blockcypher.com/btc-testnet/pushtx/>

Robin: <https://blockstream.info/testnet/tx/push>




9. After Broadcasting we can observe both transactions. We can clearly see the double spending attack apparent by the warning message on Batman's transaction.

 **Transaction** Testnet


ef46554e8b76d79df3f47b712d4236f9391cd9840bc13ba7ed0150d1993edeb0 




STATUS	Unconfirmed
ETA	in 1 blocks (0.00 vMB from tip)
TRANSACTION FEES	0.00000565 tBTC (5.0 sat/vB) <span>⚠ overpaying by 403%</span>
SIZE	194 B
VIRTUAL SIZE	113 vB
WEIGHT UNITS	449 WU
VERSION	2
LOCK TIME	0
REPLACE BY FEE	Opted in
SEGWIT FEE SAVINGS	This transaction saved 41% on fees by upgrading to native SegWit-Bech32
PRIVACY ANALYSIS	Possibly self-transfer ✓


ef46554e8b76d79df3f47b712d4236f9391cd9840bc13ba7ed0150d1993edeb0 DETAILS +

 c80367b1a7feea8831abeea3c584aef19361c76cb0f603865a11dc2aaa4 0.0370542 tBTC  
67042:1


>

 mio1EaCc7fHhNZqqDC4x826UTAE6RoBIN 0.03704855 tBTC

 **BLOCKCYPHER** BTC Testnet   

 **Bitcoin Testnet Transaction**  
25f05bdebb792dfb45c060e64d44cdb6faaca3a68ec99be742646fe5bf311549

⚠ WARNING: This transaction has been double-spent by ef46554e8b76d79df3f47b712d4236f..., be extremely careful when accepting this transaction!


AMOUNT TRANSACTED <b>0.03704855 BTC</b>	FEES <b>0.00000565 BTC</b>	RECEIVED <b>⌚ 9 minutes ago</b>	CONFIRMATIONS  <b>🔒 0/6</b>
--	-------------------------------	------------------------------------	---

Size	194 bytes
Virtual Size	113 vbytes
Lock Time	
Version	2
Relayed By:	44.211.117.182

</> API Call 📄 API Docs


Details

1 Input Consumed

0.0370542 BTC from  
 tb1qxlazymn8lg7z8e9548e6xqtktfvsxgj7a325u73 (o...


...


1 Output Created

0.03704855 BTC to  
 mgz7sshZaZ57A9tUmMs1yAc2ZdesBATMAN (unsp...

(zoom in)


While waiting, we can see that Batman's valid transaction is confirmed while Robin's is not.


 Bitcoin Testnet Transaction  
25f05bdebb792dfb45c060e64d44cdb6faaca3a68ec99be742646fe5bf311549

 WARNING: This transaction has been double-spent by ef46554e8b76d79df3f47b712d4236f..., be extremely careful when accepting this transaction!

AMOUNT TRANSACTED <b>0.03704855 BTC</b>	FEES <b>0.00000565 BTC</b>	RECEIVED <b>⌚ 19 minutes ago</b>	CONFIRMATIONS ⓘ <b>🔒 2/6</b>
--	-------------------------------	-------------------------------------	---------------------------------

Advanced Details ▾

 Bitcoin Testnet Transaction  
ef46554e8b76d79df3f47b712d4236f9391cd9840bc13ba7ed0150d1993edeb0

 WARNING: This transaction has been double-spent by 25f05bdebb792dfb45c060e64d44cdb..., be extremely careful when accepting this transaction!

AMOUNT TRANSACTED <b>0.03704855 BTC</b>	FEES <b>0.00000565 BTC</b>	RECEIVED <b>⌚ 19 minutes ago</b>	CONFIRMATIONS ⓘ <b>🔒 0/6</b>
--	-------------------------------	-------------------------------------	---------------------------------

(Unfortunately transactions didn't show on Blockchain.com)

Batman: <https://live.blockcypher.com/btc-testnet/tx/25f05bdebb792dfb45c060e64d44cdb6faaca3a68ec99be742646fe5bf311549/>

Robin:

<https://live.blockcypher.com/btc-testnet/tx/ef46554e8b76d79df3f47b712d4236f9391cd9840bc13ba7ed0150d1993edeb0/>

So to explain to Commissioner Gordon, double spend attacks are practically infeasible on the Bitcoin network because of the process of validating and confirming transactions. The first transaction to be included in a block and added to the blockchain is considered valid (e.g Batman's), while any subsequent attempt to spend the same bitcoin is rejected by the network (e.g Commissioner Gordon's). This is because nodes recognize that the bitcoin has already been spent and that the subsequent transaction is attempting to double spend. The process of verifying and confirming transactions ensures that double spend attacks are not successful on the Bitcoin network.