The blockchain : Theory and Practice (CS5543)

BItcoin application using Multi-sig

POSHAM RAMESH NAIDU

CS15BTECH11030

B.Tech Final year

Bitcoin 2 of 3 Multisig :

This is an example walkthrough of using bitcoind RPC commands to generate a 2 of 3 multisignature address. We will:

- Generate three private keys
- Find the ECDSA public key for each address
- Generate a 2 of 3 multisig address
- Send coins to the multisig address
- Generate a transaction to spend funds out of the multisig address
- Sign the transaction with two of the keys
- Broadcast that transaction on the network

Installation

1. npm install
2. cd public-key-generator
3. make
4. cd ..

Steps

First we will generate some private keys. It is very important that this process is as random as possible. I'd suggest a hardware true random number generator such as the [FST-01]

node private-key-generator

You will get something like this:
Private Key in Hex: f3d03f863d9dd6ed35b9c15739f34d8c8fdd07797cc5cc6f2e610721d06bb816
Private Key in WIF: 5KffUB9YUsvoGjrcn76PjVnC61PcWLzws4QPfrT9RFNd85utCkZ

Here, WIF stands for Wallet Import Format - a bitcoin specific way of representing an address which includes a checksum capability.

Now we want to generate a total of three private keys. The Other two are:
Private Key in Hex: e919e62a30f8ca06b66d7c9c22c176c77646c3db2c06d3ed1db0a9b2cc9f4b58
Private Key in WIF: 5KawqZHB1H6Af12ZhgTBXwQUY1jACgvGMywET7NF5bdYYzCxomY

Private Key in Hex: f99974355fbe8865e522643421914acb8f3efc0e3a1a746aa2fe68993e700d4e
Private Key in WIF: 5KiDGG8sfmTNnzKDmm1MteWHV2TQQaUBbaEY3huVLwVz1i6i5be

Now we want to generate a ECDSA(Elliptic Curve Digital Signature Algorithm) public key that corresponds to each of the private keys. Let's use the hex value of each private key to find an associated ECDSA public key:

cd public-key-generator
./ecdsapubkey f3d03f863d9dd6ed35b9c15739f34d8c8fdd07797cc5cc6f2e610721d06bb816
04A97B658C114D77DC5F71736AB78FBE408CE632ED1478D7EAA106EEF67C55D58A91C6449DE4858FAF
11721E85FE09EC850C6578432EB4BE9A69C76232AC593C3B

./ecdsapubkey e919e62a30f8ca06b66d7c9c22c176c77646c3db2c06d3ed1db0a9b2cc9f4b58
04019EF04A316792F0ECBE5AB1718C833C3964DEE3626CFABE19D97745DBCAA5198919081B456E8EEEA
5898AFA0E36D5C17AB693A80D728721128ED8C5F38CDBA0

./ecdsapubkey f99974355fbe8865e522643421914acb8f3efc0e3a1a746aa2fe68993e700d4e
04A04F29F308160E6F945B33D943304B1B471ED8F9EACEEB5412C04E60A0FAB0376871D9D1108948B67
CAFBC703E565A18F8351FB8558FD7C7482D7027EECD687C

Now we will create our multisig address given the three hex public keys. The parameter "2" tells bitcoind to create an address that requires the signature of at least two private keys. The fact that we are presenting three ECDSA keys as well is what makes it a two of three address. You can use any number of keys as long as it is equal to or greater than the "minimum required to sign" parameter. Two of two and three of five are other common strategies.

bitcoin-cli createmultisig 2
'["04A97B658C114D77DC5F71736AB78FBE408CE632ED1478D7EAA106EEF67C55D58A91C6449DE4858FAF11721E85FE09EC850C6578432EB4BE9A69C76232AC593C3B","04019EF04A316792F0ECBE5AB1718C833C3964DEE3626CFABE19D97745DBCAA5198919081B456E8EEEA5898AFA0E36D5C17AB693A80D728721128ED8C5F38CDBA0","04A04F29F308160E6F945B33D943304B1B471ED8F9EACEEB5412C04E60A0FAB0376871D9D1108948B67CAFBC703E565A18F8351FB8558FD7C7482D7027EECD687C"]'

{

"address" : "38aNB81yPqNp6X2T3rXYZN8Z3C4pSbqEvs",

"redeemScript" :
"524104a97b658c114d77dc5f71736ab78fbe408ce632ed1478d7eaa106eef67c55d58a91c6449de4858faf1
1721e85fe09ec850c6578432eb4be9a69c76232ac593c3b4104019ef04a316792f0ecbe5ab1718c833c3964
dee3626cfabe19d97745dbcaa5198919081b456e8eeea5898afa0e36d5c17ab693a80d728721128ed8c5f3
8cdba04104a04f29f308160e6f945b33d943304b1b471ed8f9eaceeb5412c04e60a0fab0376871d9d110894
8b67cafbc703e565a18f8351fb8558fd7c7482d7027eecd687c53ae"

}

So in this case, our address is **38aNB81yPqNp6X2T3rXYZN8Z3C4pSbqEvs**. Let's send it some coins:

bitcoin-cli sendtoaddress 38aNB81yPqNp6X2T3rXYZN8Z3C4pSbqEvs 0.001
7e69687c94c57a878cf711a39870383c6fe93b420f26184a21d020d8ace2df83

The resulting transaction (transaction number 7e69687c94c57a878cf711a39870383c6fe93b420f26184a21d020d8ace2df83) is a spend to our new address. That transaction will show some coin going in and other coin being returned as change. We will need the vout and the scriptPubKey of the output that we can now spend. Let's take a look:

bitcoin-cli getrawtransaction
7e69687c94c57a878cf711a39870383c6fe93b420f26184a21d020d8ace2df83 1

```
{
  "value" : 0.00100000,
  "n" : 1,
  "scriptPubKey" : {
    "asm" : "OP_HASH160 4b86dfac7f503de1127366815d1d452413282466 OP_EQUAL",
    "hex" : "a9144b86dfac7f503de1127366815d1d45241328246687",
    "reqSigs" : 1,
    "type" : "scripthash",
    "addresses" : [
      "38aNB81yPqNp6X2T3rXYZN8Z3C4pSbqEvs"
    ]
  }
```

}

Let's spend that money out of the address. To do that, we'll create a spend transaction that spends away 0.0009 BTC leaving the remainder (0.0001 BTC) to cover fees for the miners.

bitcoin-cli createrawtransaction

'[{"txid":"7e69687c94c57a878cf711a39870383c6fe93b420f26184a21d020d8ace2df83","vout":1}]'
'{"19ijkHfTosmo6rHtVKte145XPnQQNqVn46":0.0009}'
010000000183dfe2acd820d0214a18260f423be96f3c387098a311f78c877ac5947c68697e0100000000ffffff
ff01905f0100000000001976a9145fa5be58f939d6ae79636c2143fa9e7924102c1588ac00000000

the JSON here is very picky. For example, it doesn't tolerate things like spaces after commas and other standard patterns. Also be careful to escape things properly in the shell. If you get stuck, try copying the example EXACTLY and just replace the transaction id and multi-sig address.

Now we have an unsigned raw transaction. It means nothing right now and can safely be sent through untrusted mediums such as unencrypted email. Let's go sign it with one of the private keys. In this case we will use the private key in Wallet Import Format. (WIF)

When doing this using the `bitcoin-abc` Bitcoin Cash (BCH / BCC) or `bgold-cli` Bitcoin Gold (BTG) you will need to also add an `amount` property to each input specifying the amount of each input. (the original input value without subtracting miner's fees) The JSON will look something like `..."vout":1,amount:0.001,"scriptPubKey"...`.

bitcoin-cli signrawtransaction

'010000000183dfe2acd820d0214a18260f423be96f3c387098a311f78c877ac5947c68697e0100000000ffffff
fff01905f0100000000001976a9145fa5be58f939d6ae79636c2143fa9e7924102c1588ac00000000'
'[{"txid":"7e69687c94c57a878cf711a39870383c6fe93b420f26184a21d020d8ace2df83","vout":1,"scriptPu
bKey":"a9144b86dfac7f503de1127366815d1d45241328246687","redeemScript":"524104a97b658c114d7
7dc5f71736ab78fbe408ce632ed1478d7eaa106eef67c55d58a91c6449de4858faf11721e85fe09ec850c657
8432eb4be9a69c76232ac593c3b4104019ef04a316792f0ecbe5ab1718c833c3964dee3626cfabe19d97745
dbcaa5198919081b456e8eeea5898afa0e36d5c17ab693a80d728721128ed8c5f38cdba04104a04f29f3081
60e6f945b33d943304b1b471ed8f9eaceeb5412c04e60a0fab0376871d9d1108948b67cafbc703e565a18f8

351fb8558fd7c7482d7027eecd687c53ae"}]'
'["5KffUB9YUsvoGjrcn76PjVnC61PcWLzws4QPfrT9RFNd85utCkZ"]'
{

"hex":"010000000183dfe2acd820d0214a18260f423be96f3c387098a311f78c877ac5947c68697e01000000fd150100483045022100acb79a21e7e6cea47a598254e02639f87b5fa9a08c0ec8455503da0a479c19560220724014c241ac64ffc108d4457302644d5d057fbc4f2edbf33a86f24cf0b10447014cc9524104a97b658c114d77dc5f71736ab78fbe408ce632ed1478d7eaa106eef67c55d58a91c6449de4858faf11721e85fe09ec850c6578432eb4be9a69c76232ac593c3b4104019ef04a316792f0ecbe5ab1718c833c3964dee3626cfabe19d97745dbcaa5198919081b456e8eeea5898afa0e36d5c17ab693a80d728721128ed8c5f38cdba04104a04f29f308160e6f945b33d943304b1b471ed8f9eaceeb5412c04e60a0fab0376871d9d1108948b67cafbc703e565a18f8351fb8558fd7c7482d7027eecd687c53aeffffffff01905f0100000000001976a9145fa5be58f939d6ae79636c2143fa9e7924102c1588ac00000000",
  "complete" : false
}

The resulting transaction in hex format is a bit longer but still marked as incomplete because we only have one signature on it. Likewise, it can be sent through insecure mediums such as email because it isn't completely signed. Even if it were, an abuser wouldn't be able to alter the transaction sending the coin to another address because that would invalidate the original signature.

However, I should point out that the transaction isn't encrypted. Let's take a look at it to demonstrate that.

bitcoin-cli decoderawtransaction

'010000000183dfe2acd820d0214a18260f423be96f3c387098a311f78c877ac5947c68697e01000000fd150100483045022100acb79a21e7e6cea47a598254e02639f87b5fa9a08c0ec8455503da0a479c19560220724014c241ac64ffc108d4457302644d5d057fbc4f2edbf33a86f24cf0b10447014cc9524104a97b658c114d77dc5f71736ab78fbe408ce632ed1478d7eaa106eef67c55d58a91c6449de4858faf11721e85fe09ec850c6578432eb4be9a69c76232ac593c3b4104019ef04a316792f0ecbe5ab1718c833c3964dee3626cfabe19d97745dbcaa5198919081b456e8eeea5898afa0e36d5c17ab693a80d728721128ed8c5f38cdba04104a04f29f308160e6f945b33d943304b1b471ed8f9eaceeb5412c04e60a0fab0376871d9d1108948b67cafbc703e565a18f8351f

b8558fd7c7482d7027eecd687c53aeffffffff01905f0100000000001976a9145fa5be58f939d6ae79636c2143fa9e7924102c1588ac00000000'


```
{
  "txid" : "3312407d07de68d09eba1c9bee333aa947f46075c6f491eaeda2025c513aa45f",
  "version" : 1,
  "locktime" : 0,
  "vin" : [
    {
      "txid" : "7e69687c94c57a878cf711a39870383c6fe93b420f26184a21d020d8ace2df83",
      "vout" : 1,
      "scriptSig" : {
        "asm" : "0
3045022100acb79a21e7e6cea47a598254e02639f87b5fa9a08c0ec8455503da0a479c19560220724014c241ac64ffc108d4457302644d5d057fbc4f2edbf33a86f24cf0b1044701
524104a97b658c114d77dc5f71736ab78fbe408ce632ed1478d7eaa106eef67c55d58a91c6449de4858faf11721e85fe09ec850c6578432eb4be9a69c76232ac593c3b4104019ef04a316792f0ecbe5ab1718c833c3964dee3626cfabe19d97745dbcaa5198919081b456e8eeea5898afa0e36d5c17ab693a80d728721128ed8c5f38cdba04104a04f29f308160e6f945b33d943304b1b471ed8f9eaceeb5412c04e60a0fab0376871d9d1108948b67cafbc703e565a18f8351fb8558fd7c7482d7027eecd687c53ae",
        "hex" :
"00483045022100acb79a21e7e6cea47a598254e02639f87b5fa9a08c0ec8455503da0a479c19560220724014c241ac64ffc108d4457302644d5d057fbc4f2edbf33a86f24cf0b10447014cc9524104a97b658c114d77dc5f71736ab78fbe408ce632ed1478d7eaa106eef67c55d58a91c6449de4858faf11721e85fe09ec850c6578432eb4be9a69c76232ac593c3b4104019ef04a316792f0ecbe5ab1718c833c3964dee3626cfabe19d97745dbcaa5198919081b456e8eeea5898afa0e36d5c17ab693a80d728721128ed8c5f38cdba04104a04f29f308160e6f945b33d943304b1b471ed8f9eaceeb5412c04e60a0fab0376871d9d1108948b67cafbc703e565a18f8351fb8558fd7c7482d7027eecd687c53ae"
      },
      "sequence" : 4294967295
    }
  ],
  "vout" : [
    {
```

```
        "value" : 0.00090000,
        "n" : 0,
        "scriptPubKey" : {
          "asm" : "OP_DUP OP_HASH160 5fa5be58f939d6ae79636c2143fa9e7924102c15
OP_EQUALVERIFY OP_CHECKSIG",
          "hex" : "76a9145fa5be58f939d6ae79636c2143fa9e7924102c1588ac",
          "reqSigs" : 1,
          "type" : "pubkeyhash",
          "addresses" : [
            "19ijkHfTosmo6rHtVKte145XPnQQNqVn46"
          ]
        }
      }
  ]
}
```


Sure enough, in the vout section you can see that this is a spend of 0.00090000 BTC to 19ijkHfTosmo6rHtVKte145XPnQQNqVn46.

Moving on, let's add another signature to this transaction:

bitcoin-cli signrawtransaction


```
'010000000183dfe2acd820d0214a18260f423be96f3c387098a311f78c877ac5947c68697e01000000fd150
100483045022100acb79a21e7e6cea47a598254e02639f87b5fa9a08c0ec8455503da0a479c195602207240
14c241ac64ffc108d4457302644d5d057fbc4f2edbf33a86f24cf0b10447014cc9524104a97b658c114d77dc5
f71736ab78fbe408ce632ed1478d7eaa106eef67c55d58a91c6449de4858faf11721e85fe09ec850c6578432
eb4be9a69c76232ac593c3b4104019ef04a316792f0ecbe5ab1718c833c3964dee3626cfabe19d97745dbca
a5198919081b456e8eeea5898afa0e36d5c17ab693a80d728721128ed8c5f38cdba04104a04f29f308160e6
f945b33d943304b1b471ed8f9eaceeb5412c04e60a0fab0376871d9d1108948b67cafbc703e565a18f8351f
b8558fd7c7482d7027eecd687c53aeffffffff01905f0100000000001976a9145fa5be58f939d6ae79636c2143f
a9e7924102c1588ac00000000'
'[{"txid":"7e69687c94c57a878cf711a39870383c6fe93b420f26184a21d020d8ace2df83","vout":1,"scriptPu
bKey":"a9144b86dfac7f503de1127366815d1d45241328246687","redeemScript":"524104a97b658c114d7
7dc5f71736ab78fbe408ce632ed1478d7eaa106eef67c55d58a91c6449de4858faf11721e85fe09ec850c657
8432eb4be9a69c76232ac593c3b4104019ef04a316792f0ecbe5ab1718c833c3964dee3626cfabe19d97745
```

dbcaa5198919081b456e8eeea5898afa0e36d5c17ab693a80d728721128ed8c5f38cdba04104a04f29f3081
60e6f945b33d943304b1b471ed8f9eaceeb5412c04e60a0fab0376871d9d1108948b67cafbc703e565a18f8
351fb8558fd7c7482d7027eecd687c53ae"}]'
'["5KiDGG8sfmTNnzKDmm1MteWHV2TQQaUBbaEY3huVLwVz1i6i5be"]'
{
"hex":"010000000183dfe2acd820d0214a18260f423be96f3c387098a311f78c877ac5947c68697e0100000
0fd5d0100483045022100acb79a21e7e6cea47a598254e02639f87b5fa9a08c0ec8455503da0a479c195602
20724014c241ac64ffc108d4457302644d5d057fbc4f2edbf33a86f24cf0b10447014730440220338862b4a1
3d67415fdaac35d408bd2a6d86e4c3be03b7abc92ee769b254dbe1022043ba94f304aff774fdb957af078c9
b302425976370cc66f42ae05382c84ea5ea014cc9524104a97b658c114d77dc5f71736ab78fbe408ce632ed
1478d7eaa106eef67c55d58a91c6449de4858faf11721e85fe09ec850c6578432eb4be9a69c76232ac593c3b
4104019ef04a316792f0ecbe5ab1718c833c3964dee3626cfabe19d97745dbcaa5198919081b456e8eeea58
98afa0e36d5c17ab693a80d728721128ed8c5f38cdba04104a04f29f308160e6f945b33d943304b1b471ed8
f9eaceeb5412c04e60a0fab0376871d9d1108948b67cafbc703e565a18f8351fb8558fd7c7482d7027eecd68
7c53aeffffffff01905f0100000000001976a9145fa5be58f939d6ae79636c2143fa9e7924102c1588ac000000
00",
  "complete" : true
}

Now our transaction is marked complete. Again, an attacker can't alter the transaction without invalidating it so it is still in a reasonably safe condition. Additionally, if our private keys were to be kept in distant and secure locations, at no point were our private keys in the same place at the same time. You can see how this strategy might be better than simply splitting a private key into multiple pieces and combining them later to spend.

All that is left is to transmit our signed transaction on the network:

bitcoin-cli sendrawtransaction

010000000183dfe2acd820d0214a18260f423be96f3c387098a311f78c877ac5947c68697e01000000fd5d0
100483045022100acb79a21e7e6cea47a598254e02639f87b5fa9a08c0ec8455503da0a479c195602207240
14c241ac64ffc108d4457302644d5d057fbc4f2edbf33a86f24cf0b10447014730440220338862b4a13d6741
5fdaac35d408bd2a6d86e4c3be03b7abc92ee769b254dbe1022043ba94f304aff774fdb957af078c9b30242
5976370cc66f42ae05382c84ea5ea014cc9524104a97b658c114d77dc5f71736ab78fbe408ce632ed1478d7
eaa106eef67c55d58a91c6449de4858faf11721e85fe09ec850c6578432eb4be9a69c76232ac593c3b410401

9ef04a316792f0ecbe5ab1718c833c3964dee3626cfabe19d97745dbcaa5198919081b456e8eeea5898afa0e36d5c17ab693a80d728721128ed8c5f38cdba04104a04f29f308160e6f945b33d943304b1b471ed8f9aceeb5412c04e60a0fab0376871d9d1108948b67cafbc703e565a18f8351fb8558fd7c7482d7027eecd687c53affffffff01905f0100000000001976a9145fa5be58f939d6ae79636c2143fa9e7924102c1588ac00000000
78126ea4aaf1acd232711b1efa3dc15832bd45d89bd5718c1cd15ec57d802497

Now we should be able to see our spend transaction populate across the network. Search for [78126ea4aaf1acd232711b1efa3dc15832bd45d89bd5718c1cd15ec57d802497] in a block explorer to verify.

Note:

1.I am unable to complete the assignment perfectly and here in the report I am trying to explain how Exactly Multi-sig algorithm works .