Multisig the Easy Way

Justin Smith
https://jsmith.website
10-SEP-2019

REQUIRED MATERIALS:
1x DESKTOP with BITCOIN CORE installed and synced
1x LAPTOP with BITCOIN CORE installed and synced
1x USB memory stick

Don’t be fooled, there are a lot of frauds out there. Triple check to make sure you are using the right software:
https://bitcoin.org/en/bitcoin-core/
https://bitcoincore.org/
https://github.com/bitcoin/bitcoin

PHASE 1: HOARDING COINS

Create a multisig address so nobody is able to easily nick your stash by using keystroke loggers or other malware.

On your DESKTOP computer:

****

1. Open Bitcoin Core, then open the console. On macOS, you can find it in Help → Debug window → Console

2. Enter this command:

```
$ getnewaddress
> 37e4JZsHcQWRKZJugbnaBLfXnGKSY8oW9e
```

The output is a new ADDRESS.

3. Since you created it on your desktop, let’s call it the DESKTOP-ADDRESS. Copy the DESKTOP-ADDRESS.

4. Create a new text file called DESKTOP-ADDRESS.txt and paste the DESKTOP-ADDRESS into the file. Save the file on a removable USB memory stick.

On the LAPTOP computer:

****

Follow steps 1-3 above, but this time on your LAPTOP.

For step 4, name the text file LAPTOP-ADDRESS.txt and save the file to your removable USB memory stick.

Now you have two files on your USB drive:

1. DESKTOP-ADDRESS.txt
2. LAPTOP-ADDRESS.txt

5. Enter this command, copy and paste the LAPTOP-ADDRESS AND DESKTOP-ADDRESS from the appropriate files:

```
$ addmultisigaddress 2 LAPTOP-ADDRESS DESKTOP-ADDRESS
```

You’ll get a bunch of weird text output. Look for this pattern:

```
"address": "38…………………………..",
```

6. This is your MSIG-ADDRESS. Copy the MSIG-ADDRESS.

7. Create a new file on your USB memory stick called MSIG-ADDRESS.txt and paste the MSIG-ADDRESS into this new file.

8. Now enter this command:

```
$ import address MSIG-ADDRESS
```

If you have turned on pruning (you have if you want to only use 550MB of disk space instead of 280GB), then you will need to perform a partial rescan. Enter this command:

```
$ getblockchaininfo
```

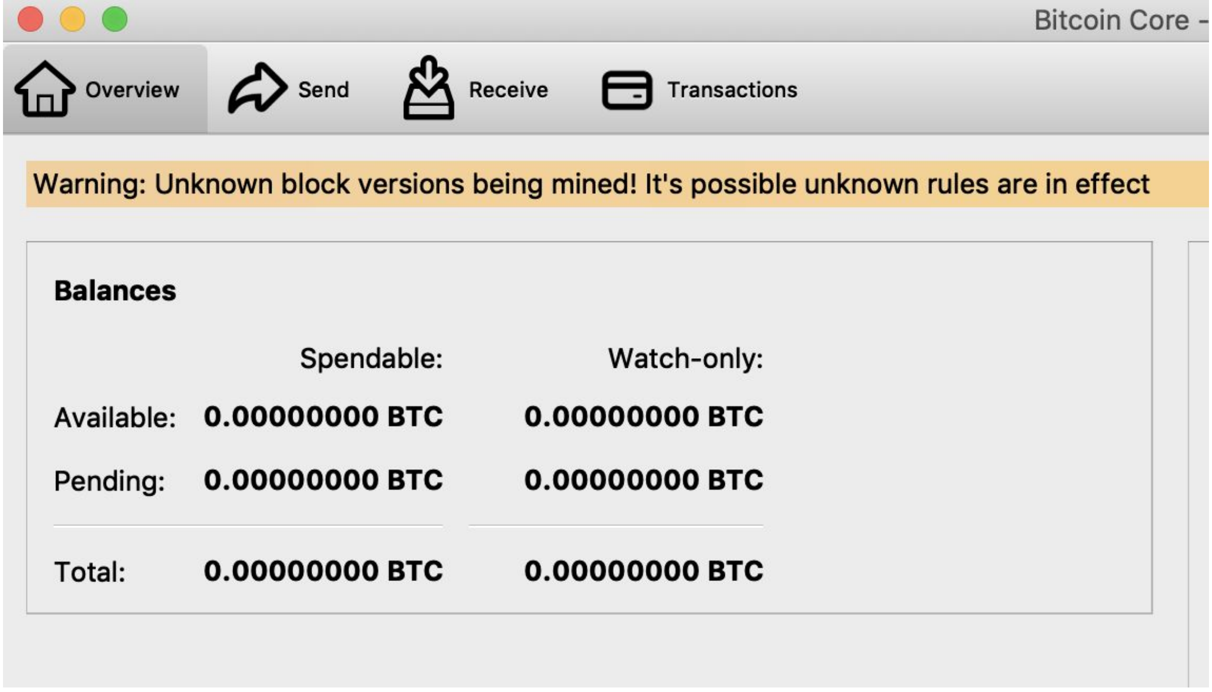
Look for this pattern:

```
"blocks": 594129,
```

Your number will be different. This number is your STOP-HEIGHT. Subtract 100 from this number. In this example (594129 - 100) = 594029. This number is your START-HEIGHT.

```
$ rescanblockchain START-HEIGHT STOP-HEIGHT
```

Now you should see something new appear in your “Overview” screen, a “Watch-only” column:



Warning: Unknown block versions being mined! It's possible unknown rules are in effect

Balances

	Spendable:	Watch-only:
Available:	**0.00000000 BTC**	**0.00000000 BTC**
Pending:	**0.00000000 BTC**	**0.00000000 BTC**
Total:	**0.00000000 BTC**	**0.00000000 BTC**

It’s like unlocking a secret in a videogame. You’ve got a new super power now: multisig.

On your DESKTOP computer:

****

Repeat Steps 6 - 8 above, copying the MSIG file from your USB memory stick. You now have the same MSIG address as a watch-only address on both your laptop and desktop machines.

Now you can send coins to the MSIG address, just like you would any other address.

PHASE 2: SPENDING YOUR HOARD

First, figure out which address you want to send coins to, and how much you want to send. This address is called the RECEIVER. In this simple example, ALL OF THE COINS LOCKED IN MULTISIG WILL BE SPENT AT ONCE.

On the LAPTOP computer:

****

1. Enter this command in your Bitcoin Core console:

```
$ listunspent
```

You’ll look for three items:

```
> txid
> vout
> amount
```

2. Enter this command:

```
$ estimatesmartfee 6
```

Look for this pattern:

```
"feerate": 0.00001026,
```

The number is your MINER-FEE. You can always optimize this number. The smaller the number, the more you’ll pay. Just don’t make the number too large or you’ll have a “stuck” transaction.

3. Subtract the miner fee from the AMOUNT you found in step 1 above. So:

(AMOUNT - MINER-FEE) = NET-AMOUNT

4. Enter this command:

```
$ createrawtransaction "[{\"txid\":\"TXID\",\"vout\":VOUT}]" "[{\"RECEIVER\":NET-AMOUNT}]"

> TXN-HEX
```

Copy the output, called the TXN-HEX.
5. If your wallet is encrypted (it should be) enter this command to unlock it:

```
        $ walletpassphrase “yourpassphrase” 120
```

Don’t worry about the plain text entry, just make sure nobody can see your screen. The text will disappear after you enter it.

6. Enter this command, pasting your TXN-HEX from your clipboard:

```
$ signrawtransactionwithwallet TXN-HEX

        “hex”: PARTIAL-SIGNATURE
```

Copy the PARTIAL-SIGNATURE. Ignore any errors that you see in the output.

6. Create a new file on your USB drive called PARTIAL-SIGNATURE.txt, and paste your PARTIAL-SIGNATURE in that file.

On your DESKTOP computer:

****

1. Open the PARTIAL-SIGNATURE file and copy the PARTIAL-SIGNATURE.
2. Follow steps 5 & 6 from above.
3. Copy the resulting output. This is called the COMPLETE-SIGNATURE.
3. Enter this command:

```
$ sendrawtransaction COMPLETE-SIGNATURE
```

You’ll notice that your “watch-only” funds are now gone. Congratulations on using multi-sig!