Running Zcash node that supports multi sig

This is a documentation of the steps I took to get zcash with 2 party shielded sapling transactions.

- Zcash original full node: https://github.com/zcash/zcash. The version I worked with is 2.0.5
- Patched zcash node: https://github.com/omershlo/zcash
- Librustzcash original repo: https://github.com/zcash/librustzcash/ . The zcash full node has hard coded the specific commit it uses of librustzcash
- The patched librustzcash: https://github.com/omershlo/librustzcash . I changed in zcash full node the hard coded commit to the latest commit in my own librustzcash. To change zcash code for newer commits this file needs to be changed: https://github.com/omershlo/zcash/blob/master/depends/packages/librustzcash.mk. Note that a sha256 of the commit need to change as well. I used this online tool: https://emn178.github.io/online-tools/sha256_checksum.html and used 'wget' to get a tar.gz file as input for the sha256: i.e. wget --no-check-certificate https://github.com/omershlo/librustzcash/archive/e3a33cba565ace9f3316a75ad1ee171cc038d874.tar.gz
- Zcash code is not using cargo update but a fixed set of signed vendored packages. To add rust libraries (not needed) this file should be updated: https://github.com/omershlo/zcash/blob/master/depends/packages/packages.mk as well as creating a .mk file for the library. I used this to add paradise city with its dependencies : https://github.com/KZen-networks/paradise-city
- To install zcash: https://zcash.readthedocs.io/en/latest/rtd_pages/user_guide.html, make sure to use the installation for the 2.0.5 version (currently latest).
- zcash.conf file must be edited. To support testnet or regtest. In this guide I will explain how to run on regtest:
    - Change to regtest=1 and comment out testnet.
    - Go to install zcash folder and run **./src/zcashd -nuparams=5ba81b19:0 -nuparams=76b809bb:0** (this will activate sapling from block 0)
    - I defined an alias: **alias zreg='./src/zcash-cli -regtest -rpcuser=SOME_USERNAME -rpcpassword=SOME_PASSWORD -nuparams=76b809bb:0'**
    - In another terminal go to zcash folder. We first generate blocks to get block reward: **zreg generate 101**
    - Check out which transparant address now owns 10 coins: **zreg listunspent** . We call this address T1
    - Generate new z_address: **zreg z_getnewaddress** we call this address Z1
    - Send from T1 to Z1: **zreg z_sendmany "T1" '[{"address": "Z1" ,"amount": 9.9999}]'**
    - Generate more blocks to confirm:
    - **zreg generate 101**
    - Generate new z address, call it Z2.

- Send from Z1 to Z2: **zreg z_sendmany "Z1" '[{"address": "Z2" ,"amount": 1.0}]'**

Note: If you terminate the full node you need to take the following actions before running it again:

- Delete Regtest folder (In Library/Application Support/Zcash)
- Delete keys1zcash and keys2 files from the zcash source folder

Using it (Oded)

Dependencies -

- sudo apt-get update

- `sudo apt-get install \`
- `build-essential pkg-config libc6-dev m4 g++-multilib \`
- `autoconf libtool ncurses-dev unzip git python python-zmq \`
- `zlib1g-dev wget curl bsdmainutils automake`

`MacOS:`

https://zcash.readthedocs.io/en/latest/rtd_pages/user_guide.html#installation

Download source code -

- `git clone https://github.com/KZen-networks/zcash`
- `cd zcash/`
- `./zcutil/fetch-params.sh`
- `mkdir ~/.zcash`
- `nano ~/.zcash/zcash.conf`

testnet=1
server=1
addnode=testnet.z.cash
rpcallowip=212.199.245.94
gen=1
genproclimit=1

(last 3 optional)

Build -

- `sudo ./zcutil/build.sh -j$(nproc)`

Run daemon -

- `./src/zcashd`