Relative Timelock Example (bitcoin-utils)

Create a new private key

Get the address that corresponds to that public key

Create an input sequence for a relative timelock of 10 blocks

What is the redeem script? Create it.

What is the P2SH address for that script?

Send some bitcoin to that P2SH address.

Can you see the transaction in the mempool?

Mine the transaction in a new block.

Can you find the transaction in the last block? What is the txid?

Create a new address in your wallet. You will use this address later to send all time locked funds to.

Having the redeem script you created earlier in mind, along with the txid and the new address you just generated, create a new transaction.

Use as input the output of the transaction you submitted to the blockchain earlier.

Use as output the address you just created in your wallet.

Add a small fee. A few satoshis is fine.

Create the transaction using the input and output.

Sign the input.

Create the signature.

Print the raw transaction.

Submit the transaction to the blockchain. What happens?