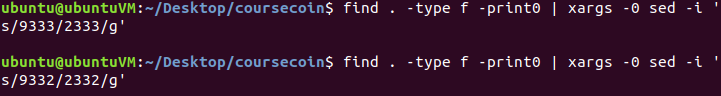
**Lab 22-08-2024**

[Note: This hands on exercise is a part of ongoing series on making your own cryptocurrency wallet, thus before doing it, please make sure that you have performed in previous labs]

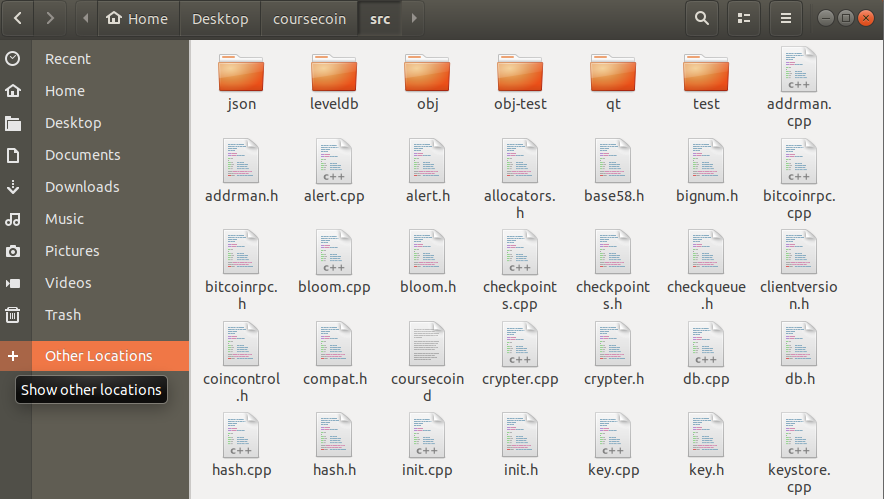
1. Open your terminal, and navigate to the directory of your coin



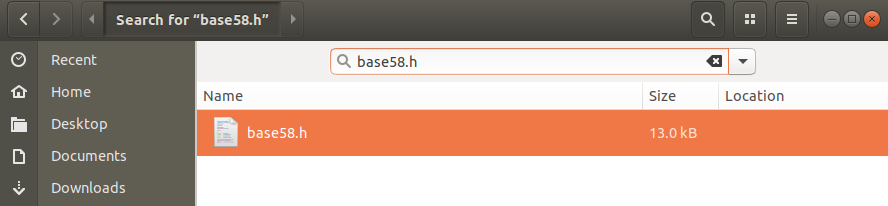
1. Type the following commands in your terminal to change the Litecoin ports to your own personal ports.
2. **find . -type f -print0 | xargs -0 sed -i 's/9333/2333/g'**
3. **find . -type f -print0 | xargs -0 sed -i 's/9332/2332/g'**

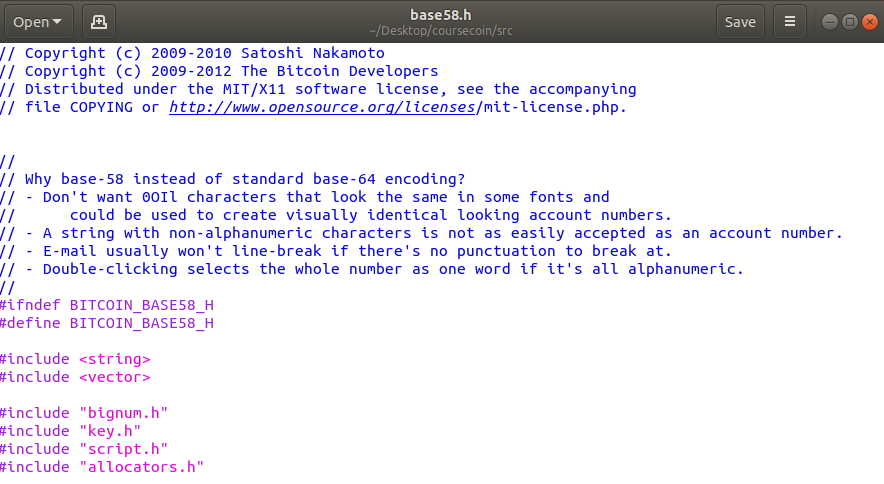


1. Go into your coin directory and into src directory

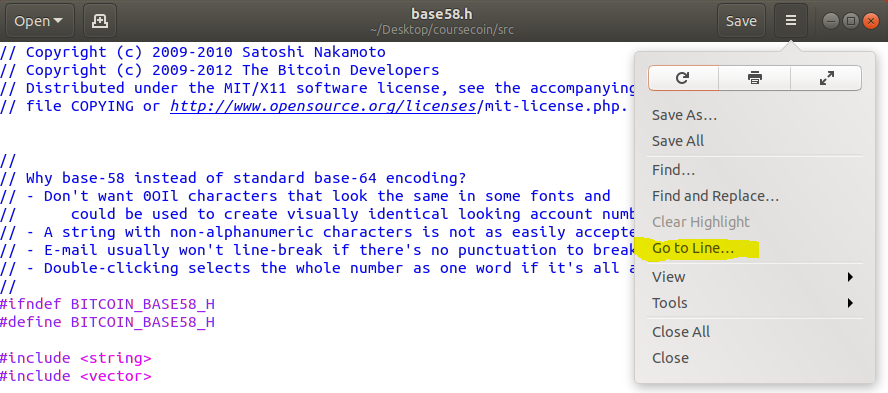


1. Search for “base58.h” in the src directory, open the file by double clicking it.

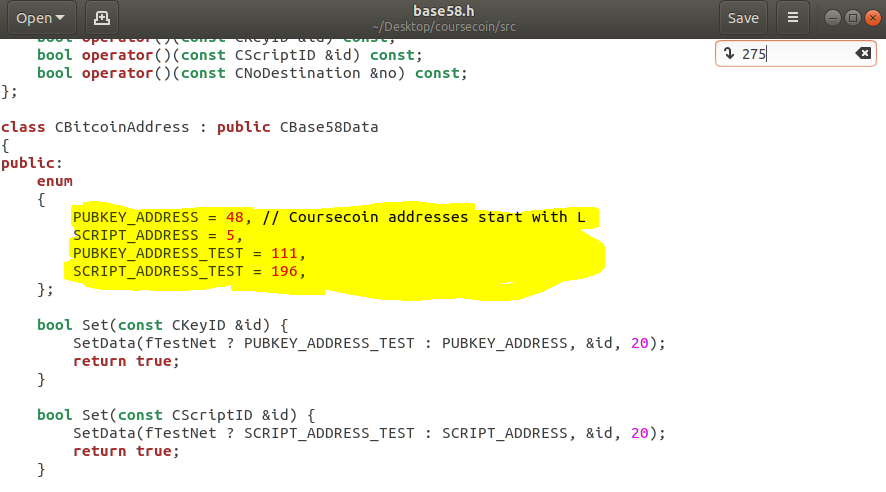




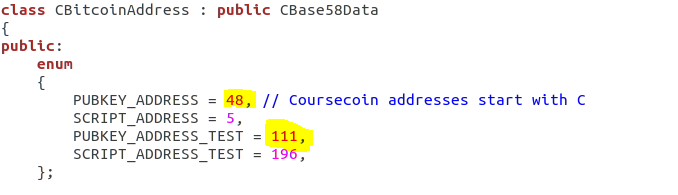
Go to line 275



You’ll see this snippet of code



We are going to change the main net and test net public key address prefixes, by changing the following highlighted numbers.

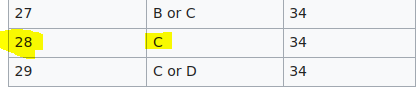


For that go to the link mentioned below

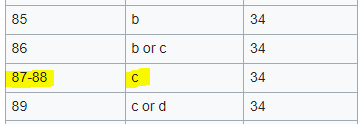
<https://en.bitcoin.it/wiki/List_of_address_prefixes>



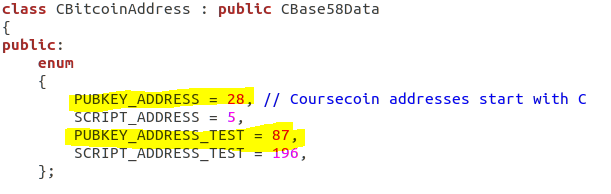
In the case of **“coursecoin”** the address for main net would start with a capital C



and for test net it would start with small letter c.



Therefore, in case of **“coursecoin”** I changed the value of PUBKEY\_ADDRESS to 28 and PUBKEY\_ADDRESS\_TEST to 87.

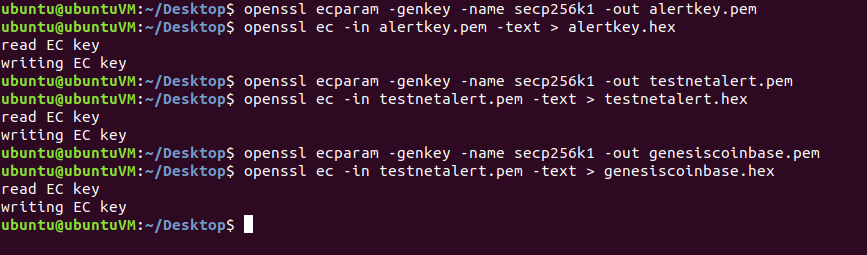


save the base58.h file and close it.

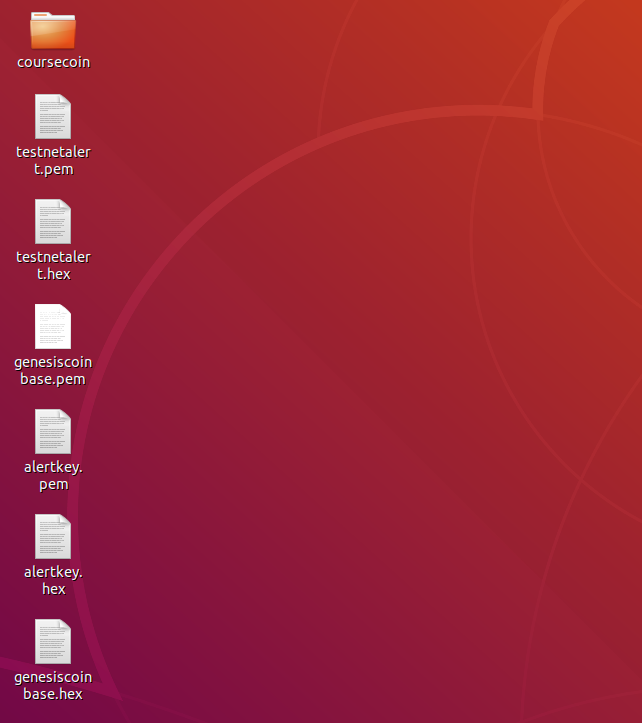
1. Open your terminal, if you are in your coin directory please navigate to your Desktop



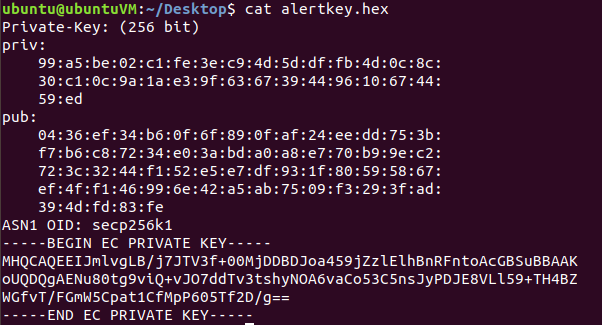
1. Type the following commands in your terminal
2. openssl ecparam -genkey -name secp256k1 -out alertkey.pem
3. openssl ec -in alertkey.pem -text > alertkey.hex
4. openssl ecparam -genkey -name secp256k1 -out testnetalert.pem
5. openssl ec -in testnetalert.pem -text > testnetalert.hex
6. openssl ecparam -genkey -name secp256k1 -out genesiscoinbase.pem
7. openssl ec -in testnetalert.pem -text > genesiscoinbase.hex



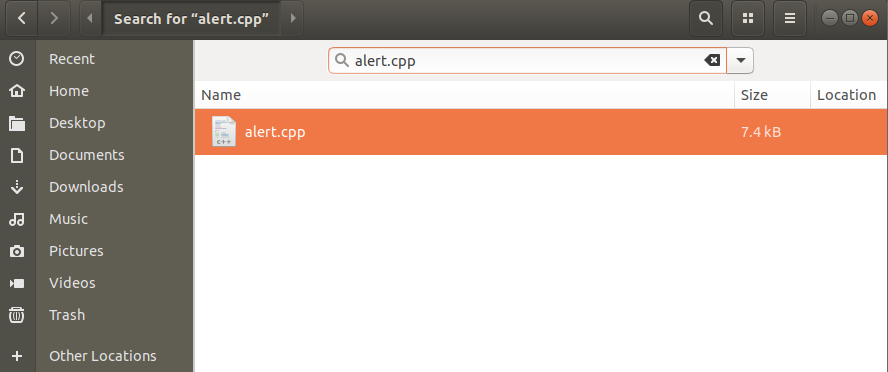
You’ll see following files on your Desktop after executing these commands.



1. Stay in your terminal and show the contents of the file named alertkey.hex by using the command **“cat alertkey.hex”**. You will see that it contained a newly generated public and private key.



Go to the src directory within your coin directory in file explorer, and search for a file named “alert.cpp” and open it.

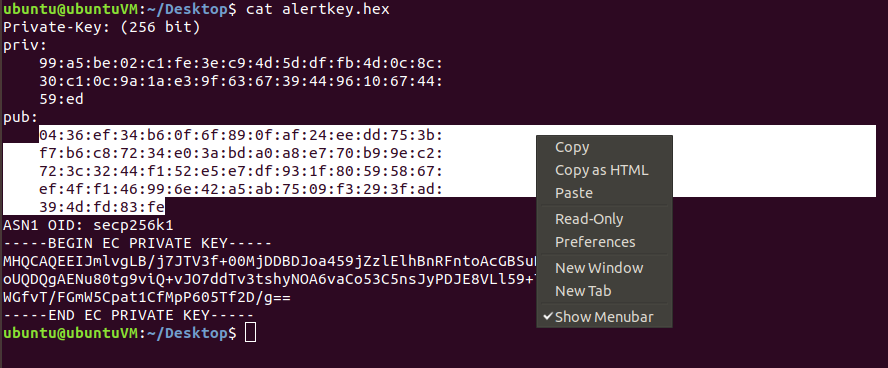




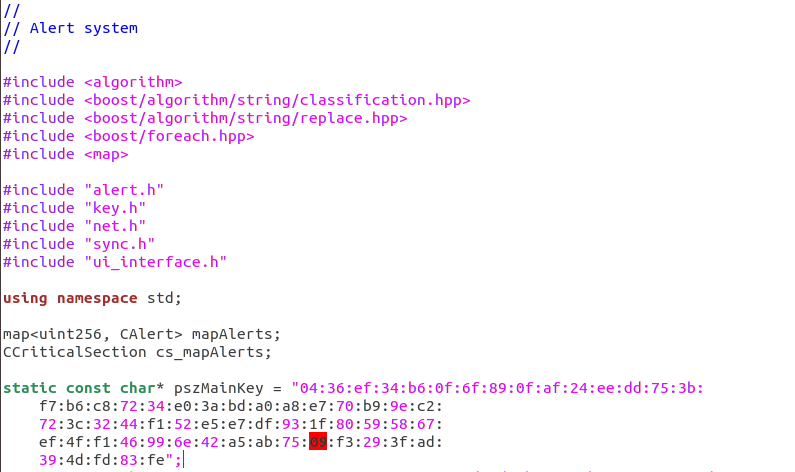
You’ll see main net and test net public keys. Erase the main net public in the file



Copy the public key that you obtained in your terminal earlier



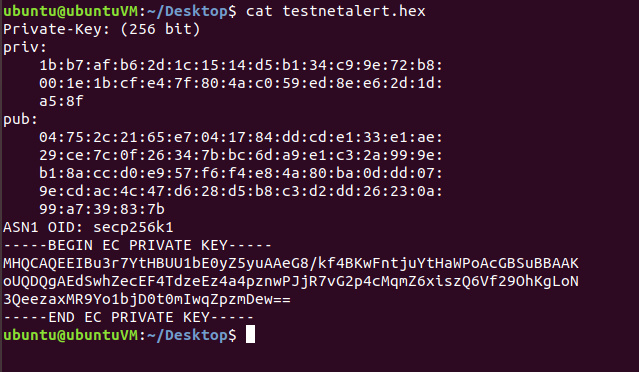
Paste it within the quotation marks



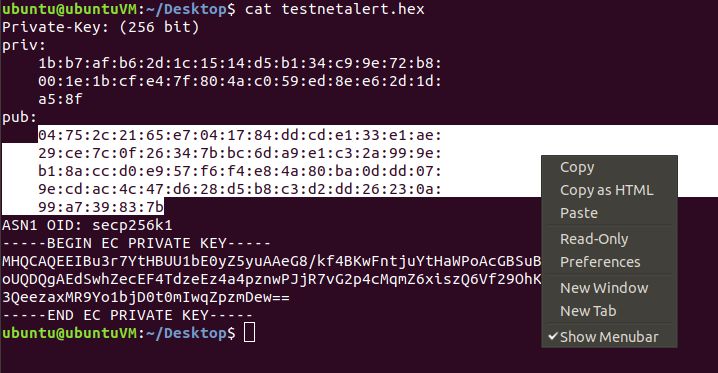
Remove every colon “:” carefully, and after removing the colons, make sure that the new main net public is of the same length as the previous test net public key below it



Save the file and go to your terminal and show the contents of the file named testnetalert.hex by typing the command “cat testnetalert.hex”.



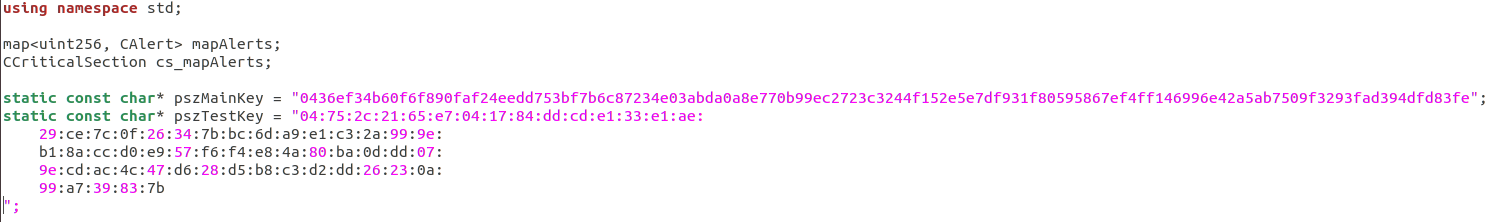
Copy the test net public key from your terminal



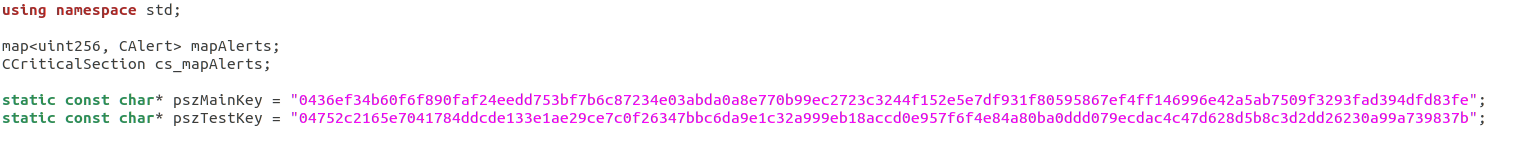
Go back to the file alert.cpp and erase the test net public key



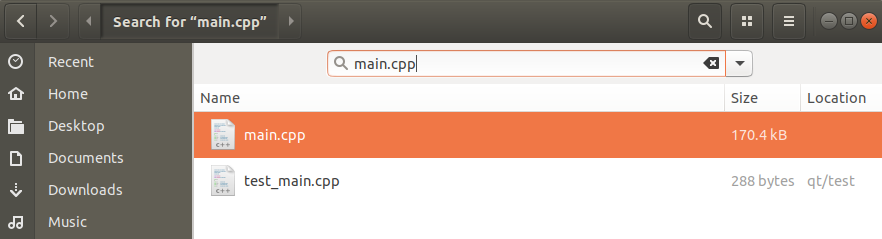
Paste the test net public key that you copied earlier



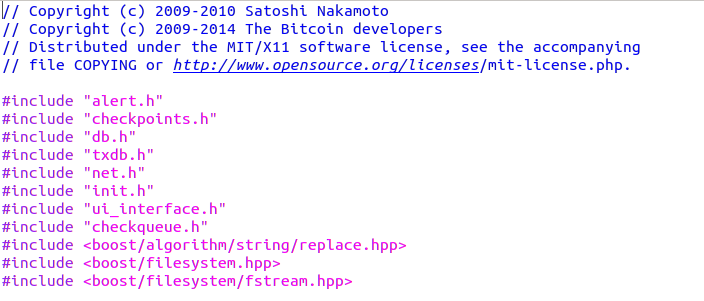
Remove every colon “:” carefully and make sure that the length of new test net public key matches the length of main net public key.



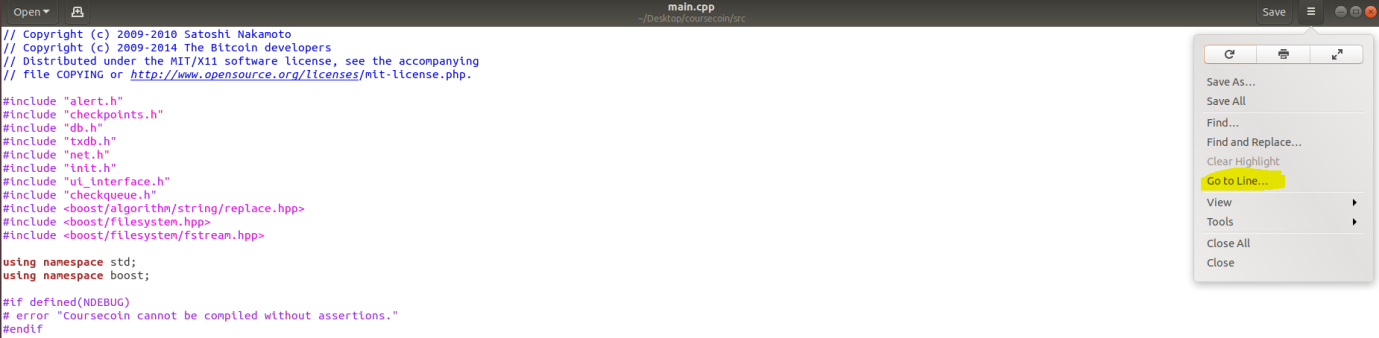
Save the file named alert.cpp and close it.

1. Now go inside your src directory within your coin directory using file explorer, and search for a file named **“main.cpp”.** 

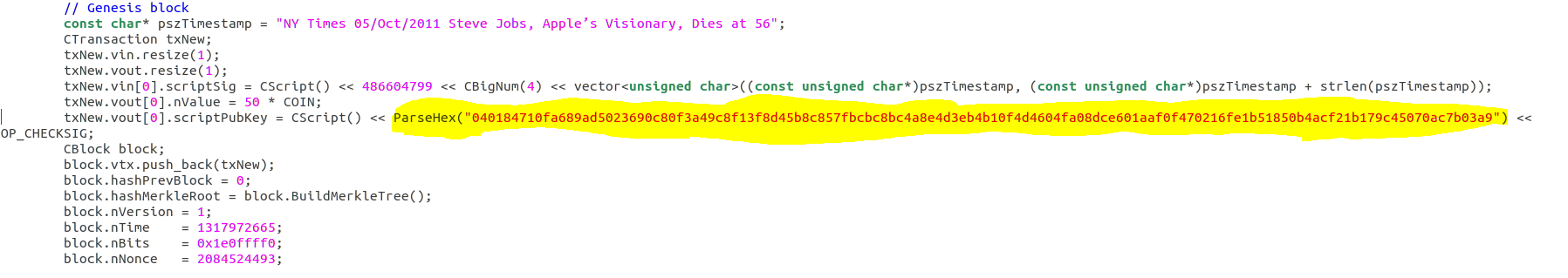
Open the file by double clicking it.



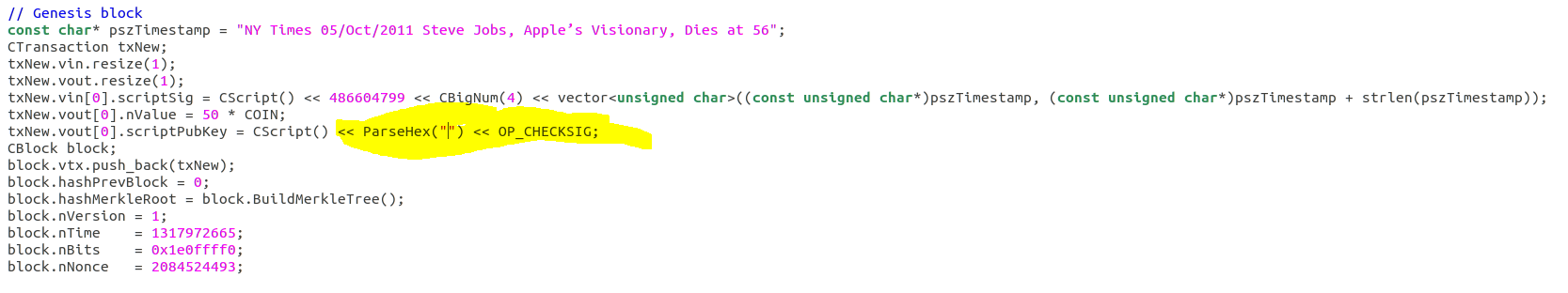
Go to line 2788



You’ll see this snippet of code; we are going to replace “ParseHex”



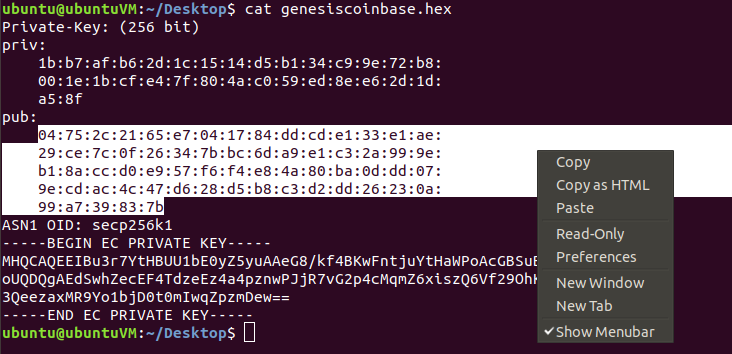
Delete the string inside ParseHex



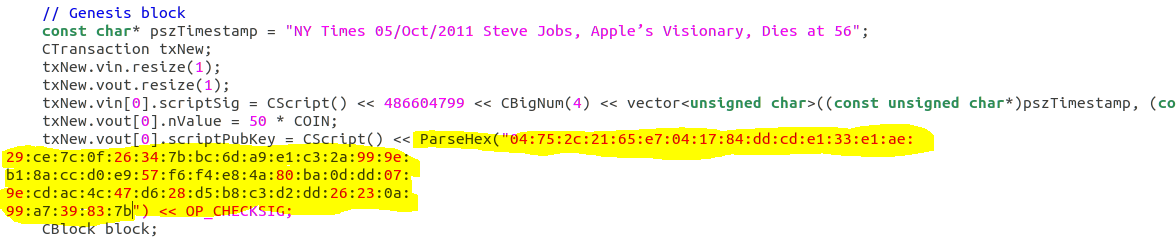
Go back to your terminal and show the contents of file named genesiscoinbase.hex by using command **“cat genesiscoinbase.hex”**.



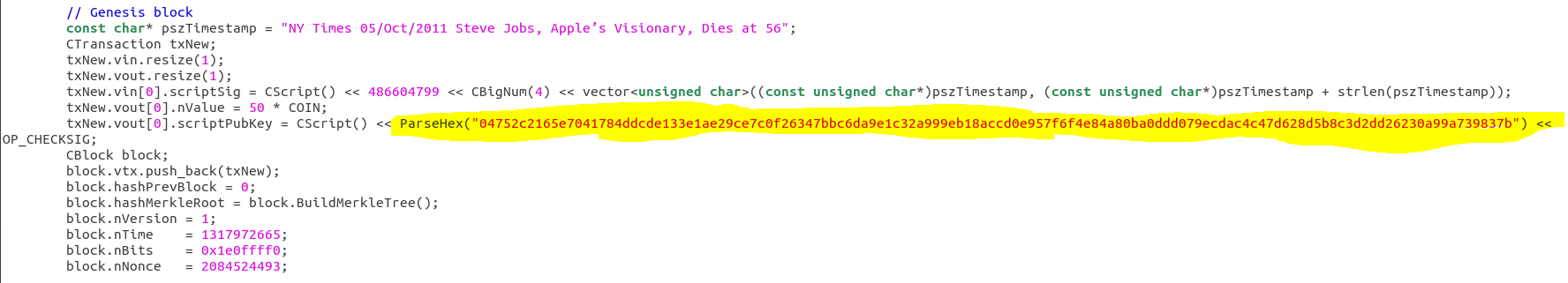
Copy the public key



And paste it in the ParseHex field.

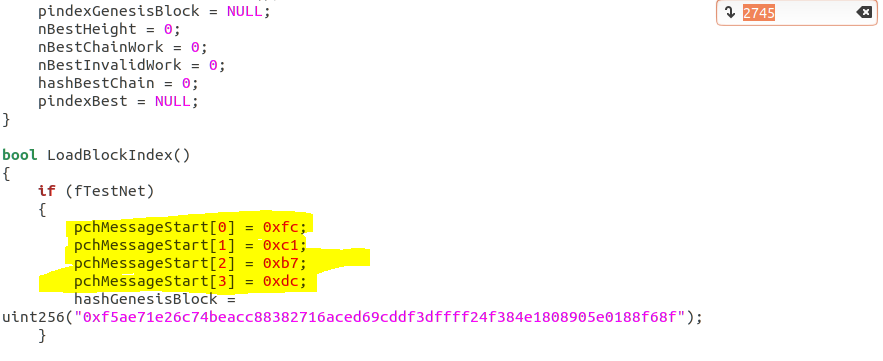


Remove the colons “:” carefully.



Once done, stay inside main.cpp for the next step.

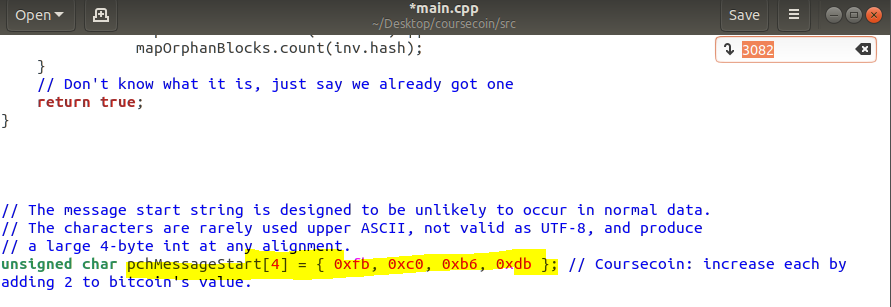
1. Go to line 2745 in main.cpp, you’ll see this snippet of code



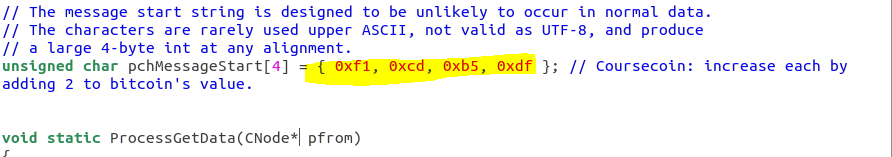
Change the last character of pchMesssageStart[0], pchMesssageStart[1], pchMesssageStart[2] and pchMesssageStart[3] randomly but please make sure that the new character is hexadecimal e.g. 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E and F.



Save the file and go to line 3082, you’ll see the following snippet of code.

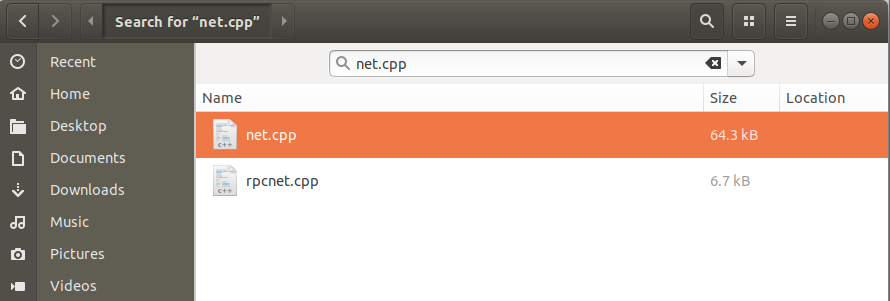


Change the last letter of pchMessageStart[4] randomly, such that it is unique to your coin. Make sure again that it is a hex number.



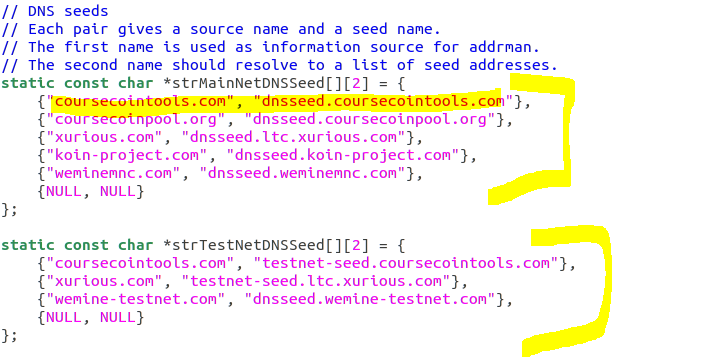
Save the main.cpp file and close it.

1. Go inside your src directory within your coin directory using file explorer and search for a file named **“net.cpp”**. Open the file by double clicking it.

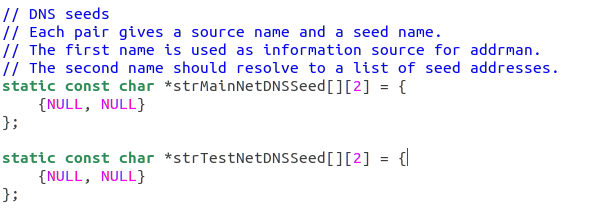




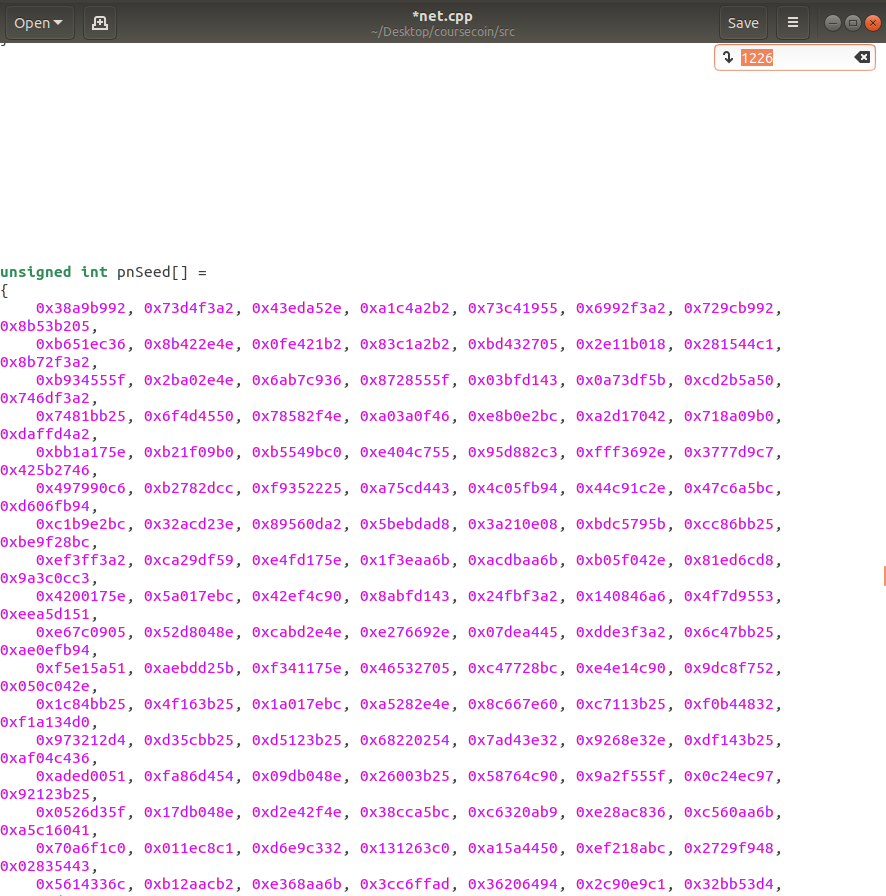
Go to line 1175 and you’ll see some main net DNS seeds and test net DNS seeds.



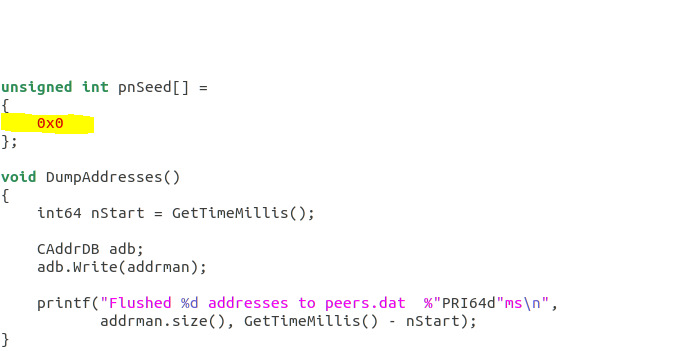
Delete all the seeds except for {NULL, NULL} in both main net and test net.



Save the file and go to line 1226, you’ll see some pnSeeds relating to Litecoin



Delete all pnSeeds and replace them by typing **“0x0”** to avoid any errors.

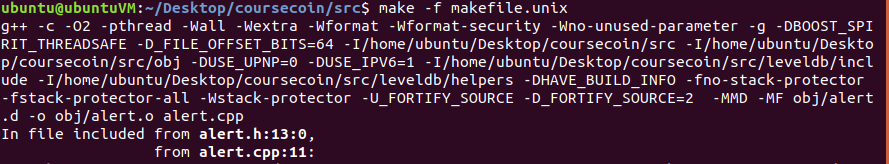


Save the net.cpp file and close it.

1. Open up your terminal, navigate to the src directory inside your coin directory.



Now to test that all of the changes that we made are working we have to compile all the files by typing the command **“make -f makefile.unix”**



If it compiles without any major error, then congratulations you are good to go for the next part. Otherwise please repeat the whole process.

1. After compilations close your VM but remember to save the machine state.