Name: Arnab Rahman Chowdhury

Find Private key from Public key and check the signature:

1 Docker container: node01-arnab

Bash to docker container:

- docker exec -it node01-arnab bash

2 Find public address of account “arnab”:

#barccoin-cli getaddressesbyaccount arnab
[
"bDpj1uiYkgSDZxDwiWZb5wzW73eEaxG6DB",
"bQE457oQ3kdqBvnQpdwgNLdFQAiJLNETEV"
]

3 Find the corresponding private key for one of the public address (base58):

#barccoin-cli dumpprivkey bDpj1uiYkgSDZxDwiWZb5wzW73eEaxG6DB
4i3cnr1RiZKTcvyaJzshqANv31XyxAENX3SFYEjuEskGZmZqcxiw

4 Validate the private key:

barccoin-cli validateaddress bDpj1uiYkgSDZxDwiWZb5wzW73eEaxG6DB

{
"isvalid": true,
"address": "bDpj1uiYkgSDZxDwiWZb5wzW73eEaxG6DB",
"scriptPubKey": "76a9140c002d9a39f2344e9897184667950b7b3671e00188ac",
"ismine": true,
"iswatchonly": false,
"isscript": false,
"pubkey": "02bab2bcbd29d0f601d9340867e9a72071662f6c9ffc2bc9c3921684b6844abd27",
"iscompressed": true,
"account": "arnab",
"timestamp": 1558049058,
"hdkeypath": "m/0'/0'/1'",
"hdmasterkeyid": "8eecb0f2064d381e48dfce75473c8c13a04cd037"
}

Here, we can find the corresponding public key of that public address:
"pubkey": "02bab2bcbd29d0f601d9340867e9a72071662f6c9ffc2bc9c3921684b6844abd27"

5 Use bitcoin-tool to convert Bitcoin keys to addresses, and various other conversions of keys:

Clone the repository:
#git clone https://github.com/matja/bitcoin-tool.git

6 Edit the prefix.c file:

Change the base58Prefixes[SECRET_KEY] in the Litecoin section of the script to the value that you used for your own coin. I have used 25 as base58Prefixes[SECRET_KEY] value.

7 Compile and run:

Make

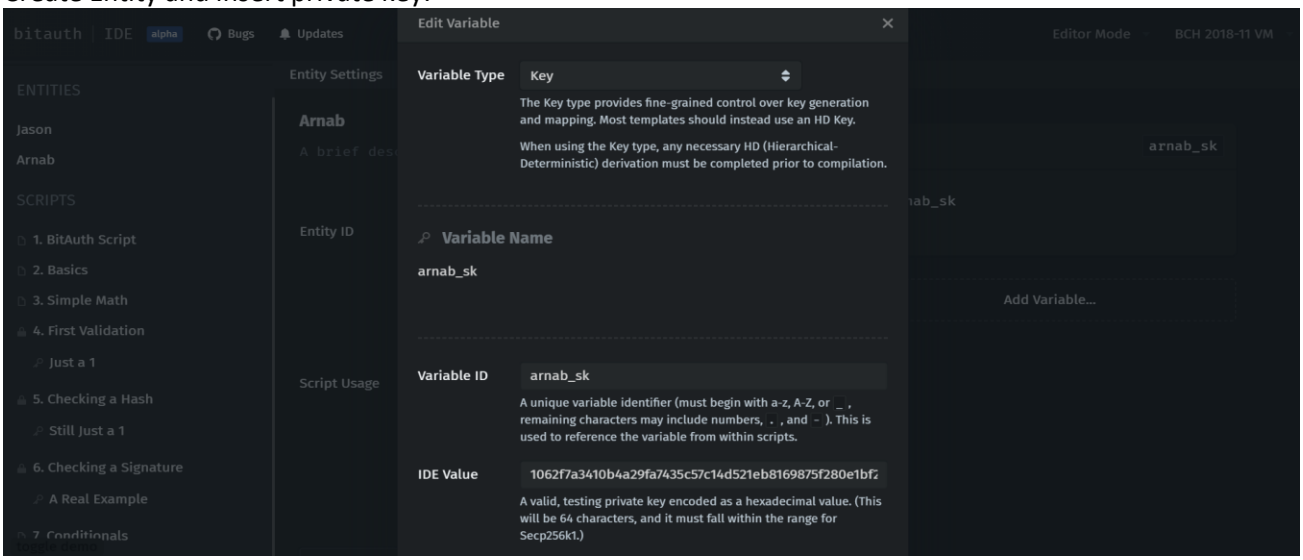
8 Run the following command to generate the 64-characters hexadecimal String:

#./bitcoin-tool --input-type private-key-wif --input-format base58check --output-type private-key --output-format hex --network litecoin --input "Base58PrivateKey"
1062f7a3410b4a29fa7435c57c14d521eb8169875f280e1bf2bc39f172514059

Base58PrivateKey=4i3cnr1RiZKTcvyaJzshqANv31XyxAENX3SFYEjuEskGZmZqcxiw

9 Go to https://ide.bitauth.com/

Create Entity and insert private key:

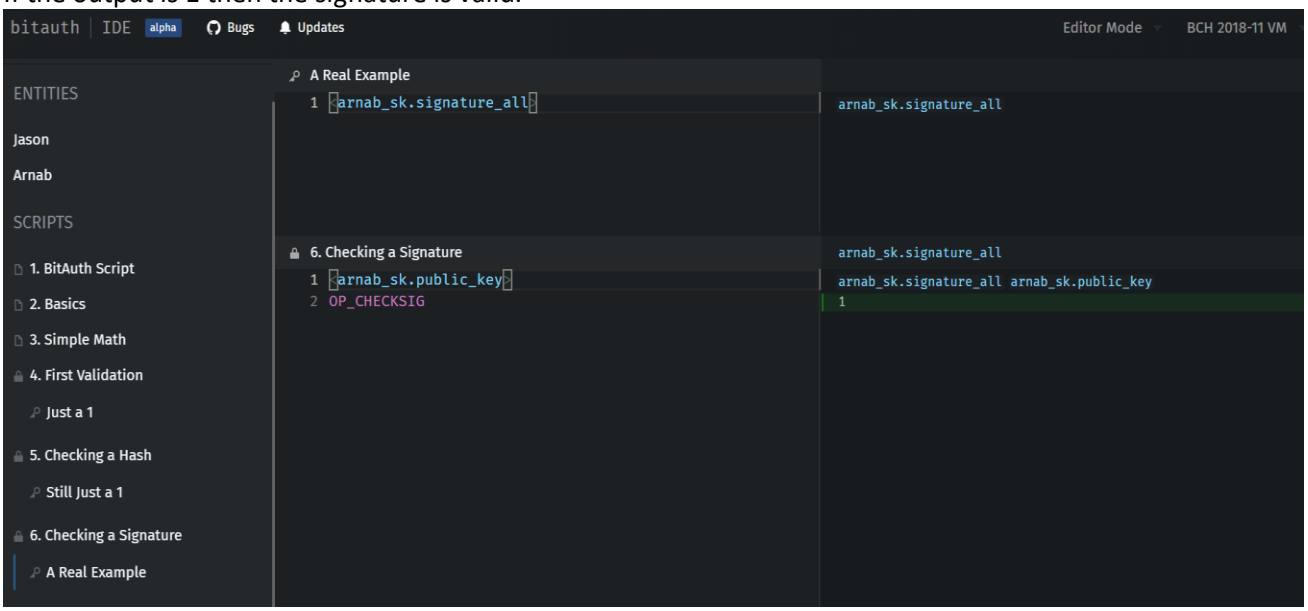


Add the name of the private key in the variable ID field and the value to IDE Value.

Variable ID: arnab_sk
IDE Value: 1062f7a3410b4a29fa7435c57c14d521eb8169875f280e1bf2bc39f172514059

10 Go to the checking signature section and verify the signature.

If the output is 1 then the signature is valid.



The arnab_sk private key match with the public key of the address that we used.