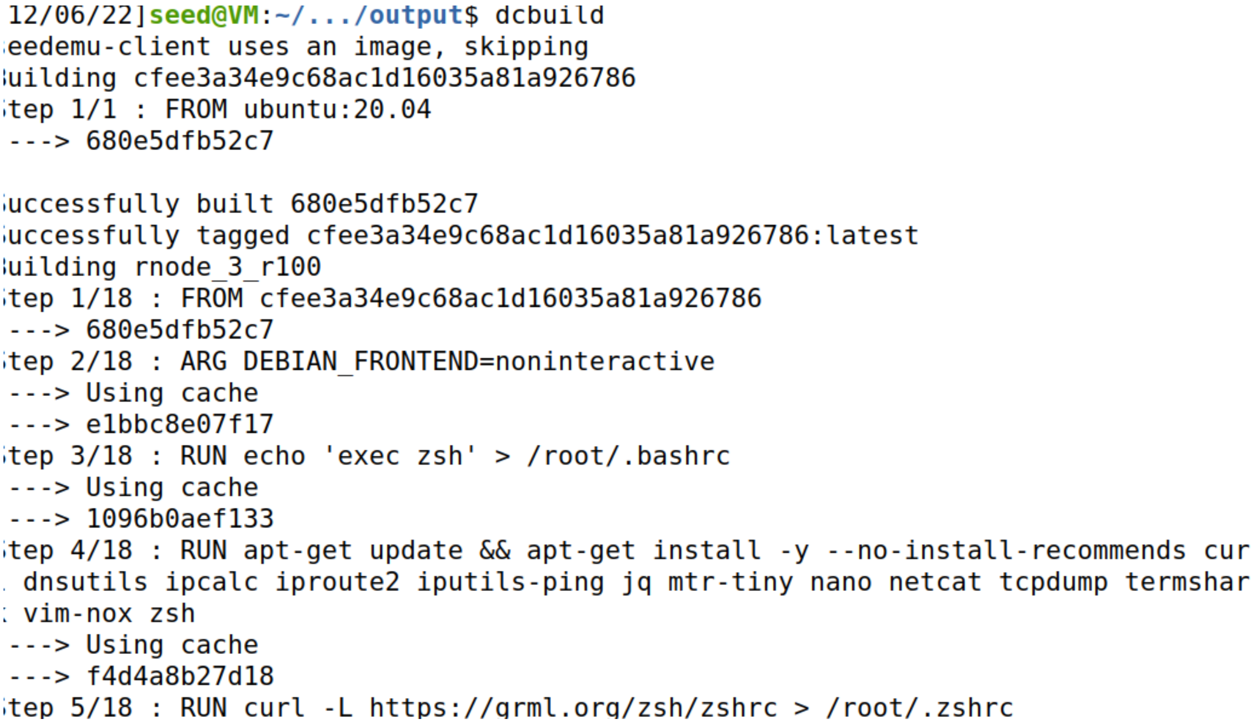
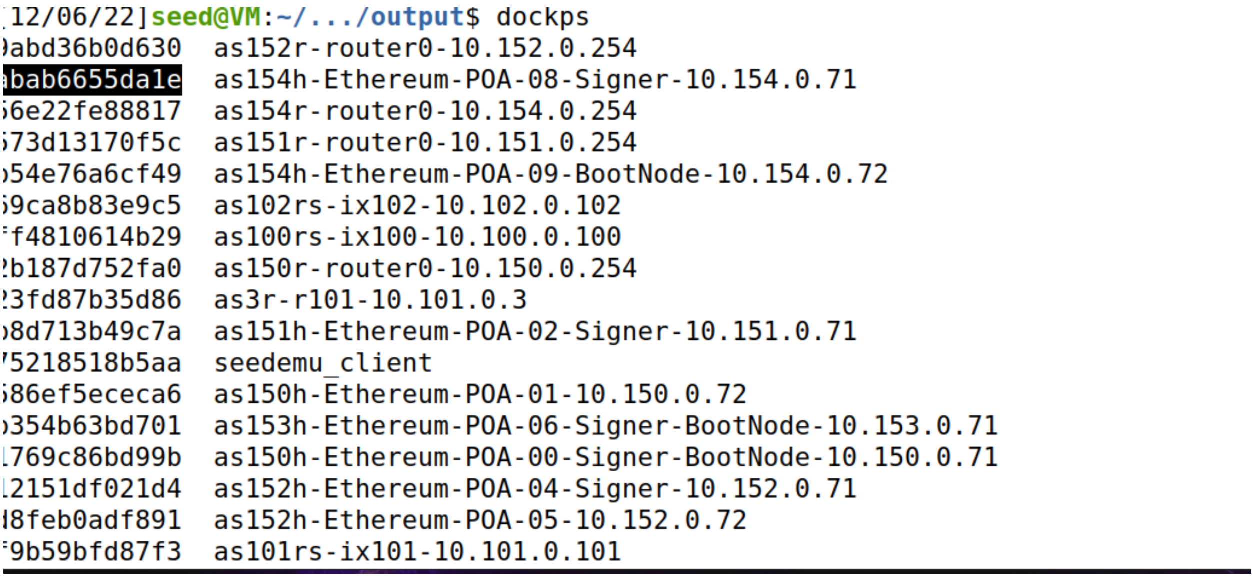
Lab-10 Blockchain Assignment 2   Henil V.   495670888

Dcbuild:



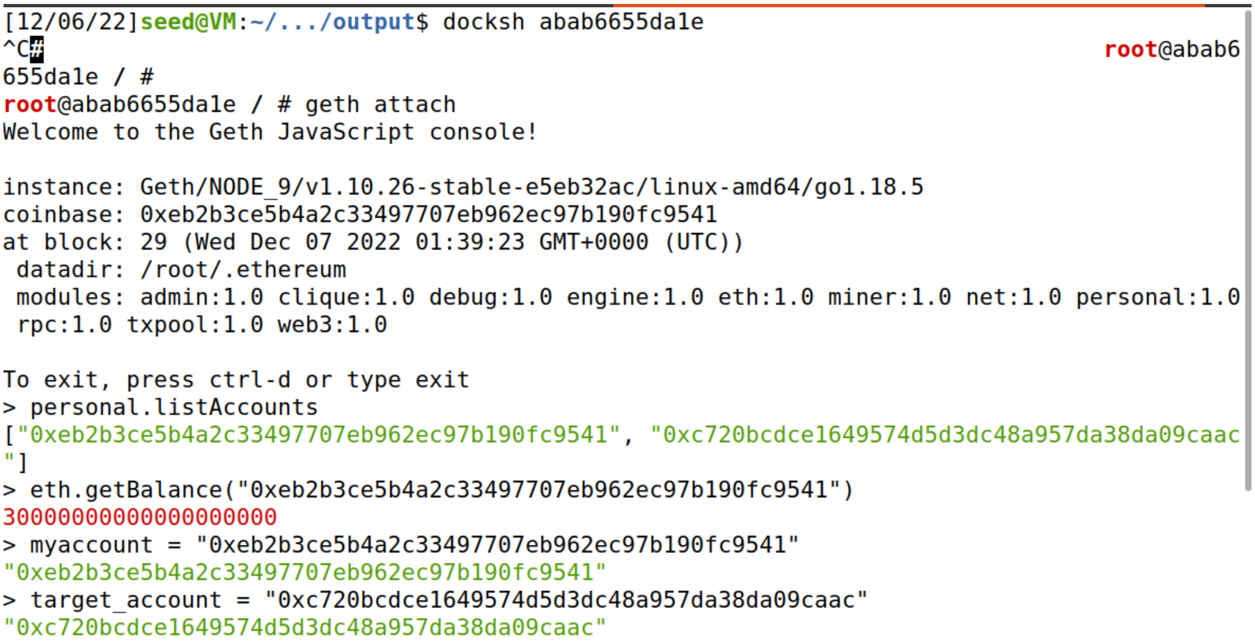
```
12/06/22]seed@VM:~/.../output$ dcbuild
eedemu-client uses an image, skipping
uilding cfee3a34e9c68ac1d16035a81a926786
tep 1/1 : FROM ubuntu:20.04
---> 680e5dfb52c7

uccessfully built 680e5dfb52c7
uccessfully tagged cfee3a34e9c68ac1d16035a81a926786:latest
uilding rnode_3_r100
tep 1/18 : FROM cfee3a34e9c68ac1d16035a81a926786
---> 680e5dfb52c7
tep 2/18 : ARG DEBIAN_FRONTEND=noninteractive
---> Using cache
---> e1bbc8e07f17
tep 3/18 : RUN echo 'exec zsh' > /root/.bashrc
---> Using cache
---> 1096b0aef133
tep 4/18 : RUN apt-get update && apt-get install -y --no-install-recommends cur
 dnsutils ipcalc iproute2 iputils-ping jq mtr-tiny nano netcat tcpdump termshar
 vim-nox zsh
---> Using cache
---> f4d4a8b27d18
tep 5/18 : RUN curl -L https://grml.org/zsh/zshrc > /root/.zshrc
```

Dcup:

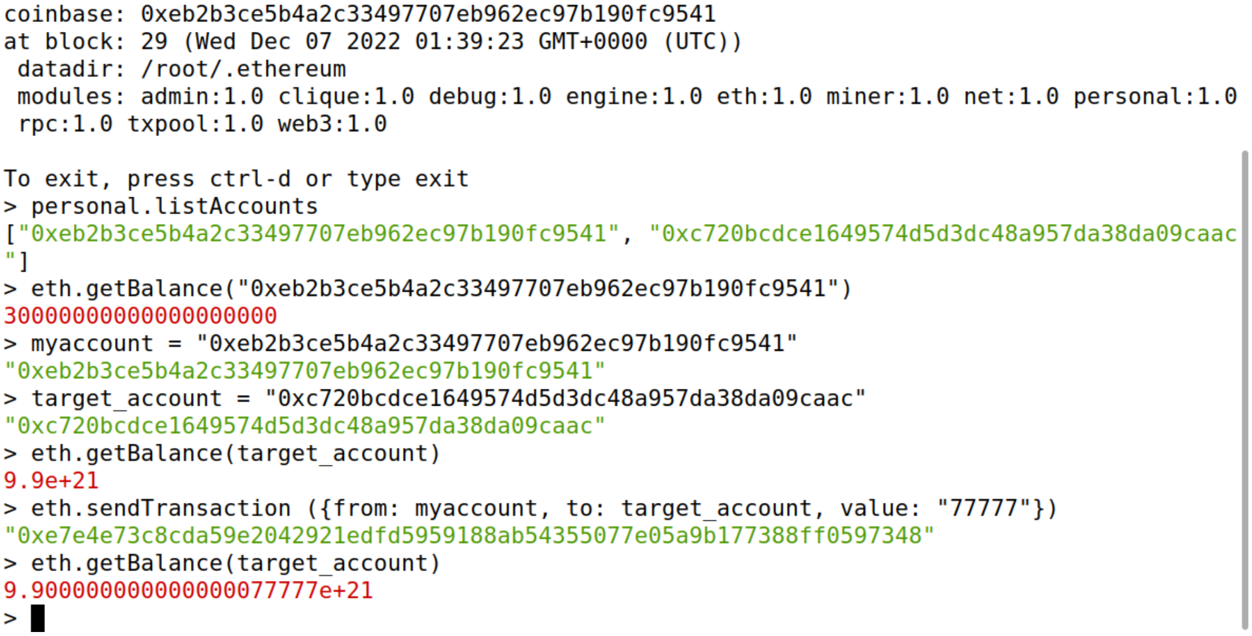


```
12/06/22]seed@VM:~/.../output$ dockps
abd36b0d630   as152r-router0-10.152.0.254
bab6655da1e   as154h-Ethereum-POA-08-Signer-10.154.0.71
6e22fe88817   as154r-router0-10.154.0.254
73d13170f5c   as151r-router0-10.151.0.254
54e76a6cf49   as154h-Ethereum-POA-09-BootNode-10.154.0.72
9ca8b83e9c5   as102rs-ix102-10.102.0.102
f4810614b29   as100rs-ix100-10.100.0.100
b187d752fa0   as150r-router0-10.150.0.254
3fd87b35d86   as3r-r101-10.101.0.3
8d713b49c7a   as151h-Ethereum-POA-02-Signer-10.151.0.71
5218518b5aa   seedemu_client
86ef5ececa6   as150h-Ethereum-POA-01-10.150.0.72
354b63bd701   as153h-Ethereum-POA-06-Signer-BootNode-10.153.0.71
769c86bd99b   as150h-Ethereum-POA-00-Signer-BootNode-10.150.0.71
2151df021d4   as152h-Ethereum-POA-04-Signer-10.152.0.71
8feb0adf891   as152h-Ethereum-POA-05-10.152.0.72
9b59bfd87f3   as101rs-ix101-10.101.0.101
```

Send Transaction:

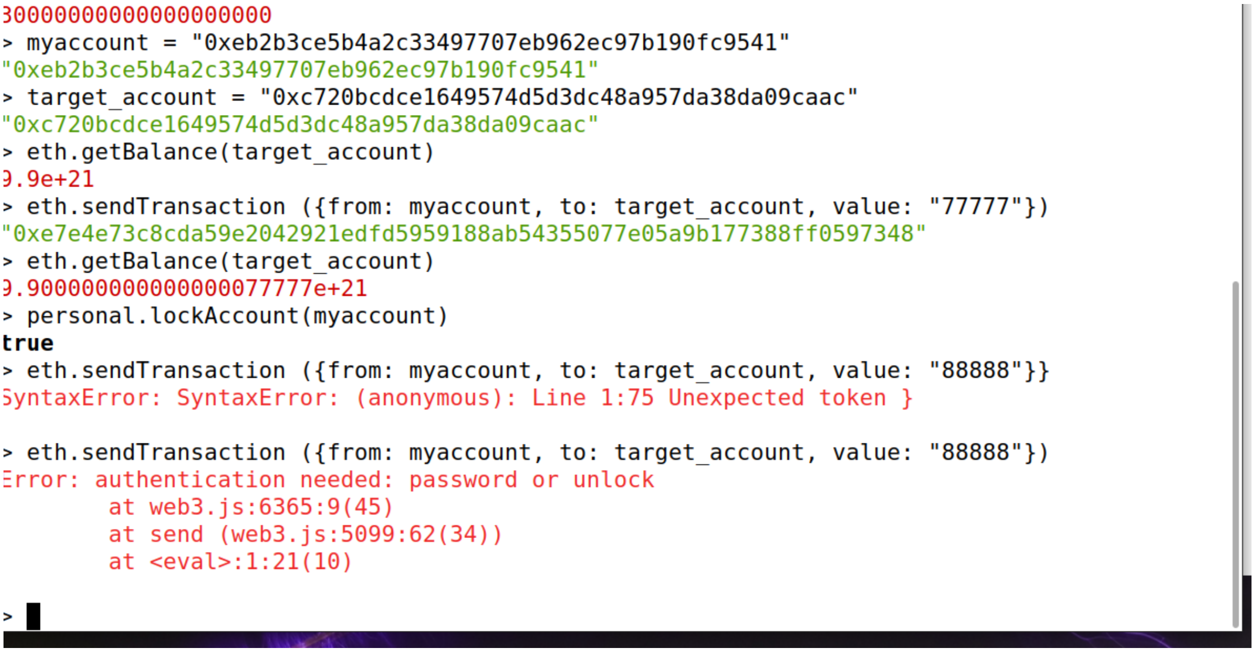


```
[12/06/22]seed@VM:~/.../output$ docksh abab6655da1e
^C#                                                                                           root@abab6
655da1e / #
root@abab6655da1e / # geth attach
Welcome to the Geth JavaScript console!

instance: Geth/NODE_9/v1.10.26-stable-e5eb32ac/linux-amd64/go1.18.5
coinbase: 0xeb2b3ce5b4a2c33497707eb962ec97b190fc9541
at block: 29 (Wed Dec 07 2022 01:39:23 GMT+0000 (UTC))
 datadir: /root/.ethereum
 modules: admin:1.0 clique:1.0 debug:1.0 engine:1.0 eth:1.0 miner:1.0 net:1.0 personal:1.0
 rpc:1.0 txpool:1.0 web3:1.0

To exit, press ctrl-d or type exit
> personal.listAccounts
["0xeb2b3ce5b4a2c33497707eb962ec97b190fc9541", "0xc720bcdce1649574d5d3dc48a957da38da09caac
"]
> eth.getBalance("0xeb2b3ce5b4a2c33497707eb962ec97b190fc9541")
30000000000000000000
> myaccount = "0xeb2b3ce5b4a2c33497707eb962ec97b190fc9541"
"0xeb2b3ce5b4a2c33497707eb962ec97b190fc9541"
> target_account = "0xc720bcdce1649574d5d3dc48a957da38da09caac"
"0xc720bcdce1649574d5d3dc48a957da38da09caac"
```



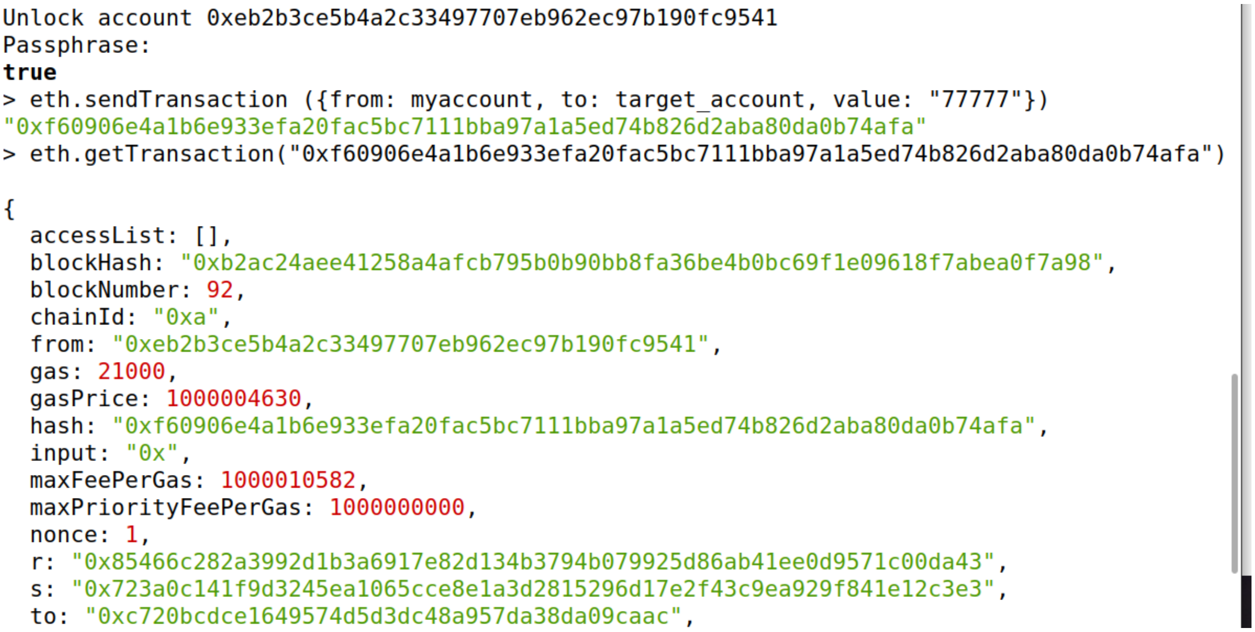
```
coinbase: 0xeb2b3ce5b4a2c33497707eb962ec97b190fc9541
at block: 29 (Wed Dec 07 2022 01:39:23 GMT+0000 (UTC))
 datadir: /root/.ethereum
 modules: admin:1.0 clique:1.0 debug:1.0 engine:1.0 eth:1.0 miner:1.0 net:1.0 personal:1.0
 rpc:1.0 txpool:1.0 web3:1.0

To exit, press ctrl-d or type exit
> personal.listAccounts
["0xeb2b3ce5b4a2c33497707eb962ec97b190fc9541", "0xc720bcdce1649574d5d3dc48a957da38da09caac
"]
> eth.getBalance("0xeb2b3ce5b4a2c33497707eb962ec97b190fc9541")
30000000000000000000
> myaccount = "0xeb2b3ce5b4a2c33497707eb962ec97b190fc9541"
"0xeb2b3ce5b4a2c33497707eb962ec97b190fc9541"
> target_account = "0xc720bcdce1649574d5d3dc48a957da38da09caac"
"0xc720bcdce1649574d5d3dc48a957da38da09caac"
> eth.getBalance(target_account)
9.9e+21
> eth.sendTransaction ({from: myaccount, to: target_account, value: "77777"})
"0xe7e4e73c8cda59e2042921edfd5959188ab54355077e05a9b177388ff0597348"
> eth.getBalance(target_account)
9.900000000000000077777e+21
> 
```

Locking Account:



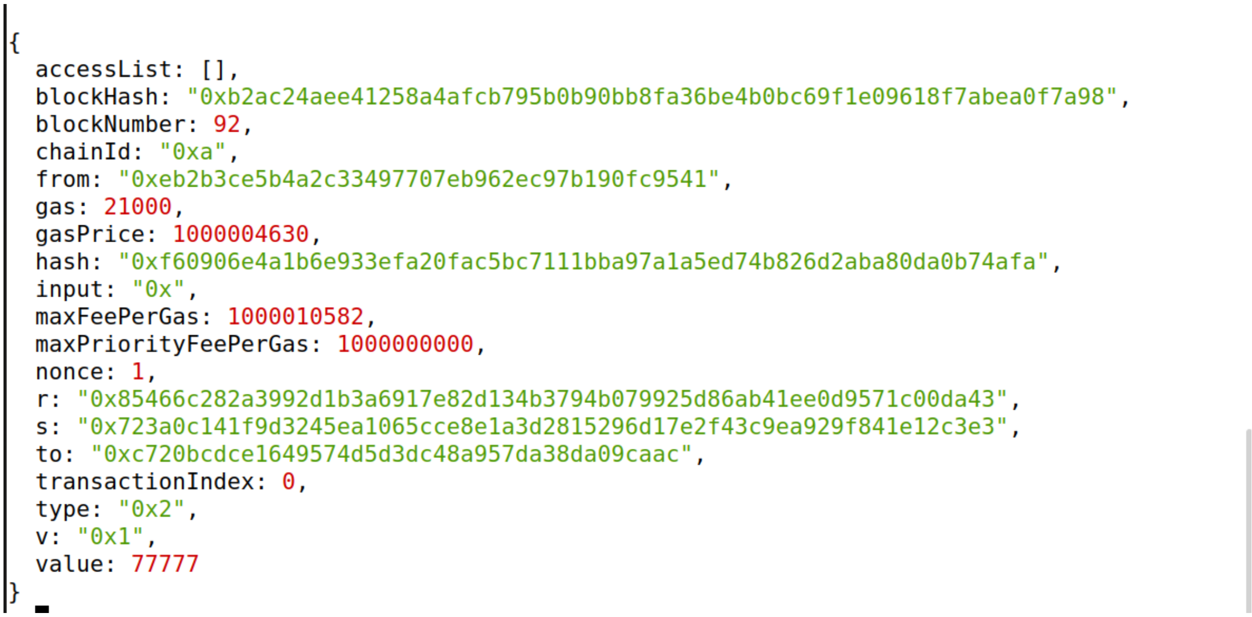
```
3000000000000000000000
> myaccount = "0xeb2b3ce5b4a2c33497707eb962ec97b190fc9541"
"0xeb2b3ce5b4a2c33497707eb962ec97b190fc9541"
> target_account = "0xc720bcdce1649574d5d3dc48a957da38da09caac"
"0xc720bcdce1649574d5d3dc48a957da38da09caac"
> eth.getBalance(target_account)
9.9e+21
> eth.sendTransaction ({from: myaccount, to: target_account, value: "77777"})
"0xe7e4e73c8cda59e2042921edfd5959188ab54355077e05a9b177388ff0597348"
> eth.getBalance(target_account)
9.900000000000000077777e+21
> personal.lockAccount(myaccount)
true
> eth.sendTransaction ({from: myaccount, to: target_account, value: "88888"}}
SyntaxError: SyntaxError: (anonymous): Line 1:75 Unexpected token }

> eth.sendTransaction ({from: myaccount, to: target_account, value: "88888"})
Error: authentication needed: password or unlock
        at web3.js:6365:9(45)
        at send (web3.js:5099:62(34))
        at <eval>:1:21(10)

> 
```

Unlock Account and Transaction Detail:



```
Unlock account 0xeb2b3ce5b4a2c33497707eb962ec97b190fc9541
Passphrase:
true
> eth.sendTransaction ({from: myaccount, to: target_account, value: "77777"})
"0xf60906e4a1b6e933efa20fac5bc7111bba97a1a5ed74b826d2aba80da0b74afa"
> eth.getTransaction("0xf60906e4a1b6e933efa20fac5bc7111bba97a1a5ed74b826d2aba80da0b74afa")

{
  accessList: [],
  blockHash: "0xb2ac24aee41258a4afcb795b0b90bb8fa36be4b0bc69f1e09618f7abea0f7a98",
  blockNumber: 92,
  chainId: "0xa",
  from: "0xeb2b3ce5b4a2c33497707eb962ec97b190fc9541",
  gas: 21000,
  gasPrice: 1000004630,
  hash: "0xf60906e4a1b6e933efa20fac5bc7111bba97a1a5ed74b826d2aba80da0b74afa",
  input: "0x",
  maxFeePerGas: 1000010582,
  maxPriorityFeePerGas: 1000000000,
  nonce: 1,
  r: "0x85466c282a3992d1b3a6917e82d134b3794b079925d86ab41ee0d9571c00da43",
  s: "0x723a0c141f9d3245ea1065cce8e1a3d2815296d17e2f43c9ea929f841e12c3e3",
  to: "0xc720bcdce1649574d5d3dc48a957da38da09caac",
```

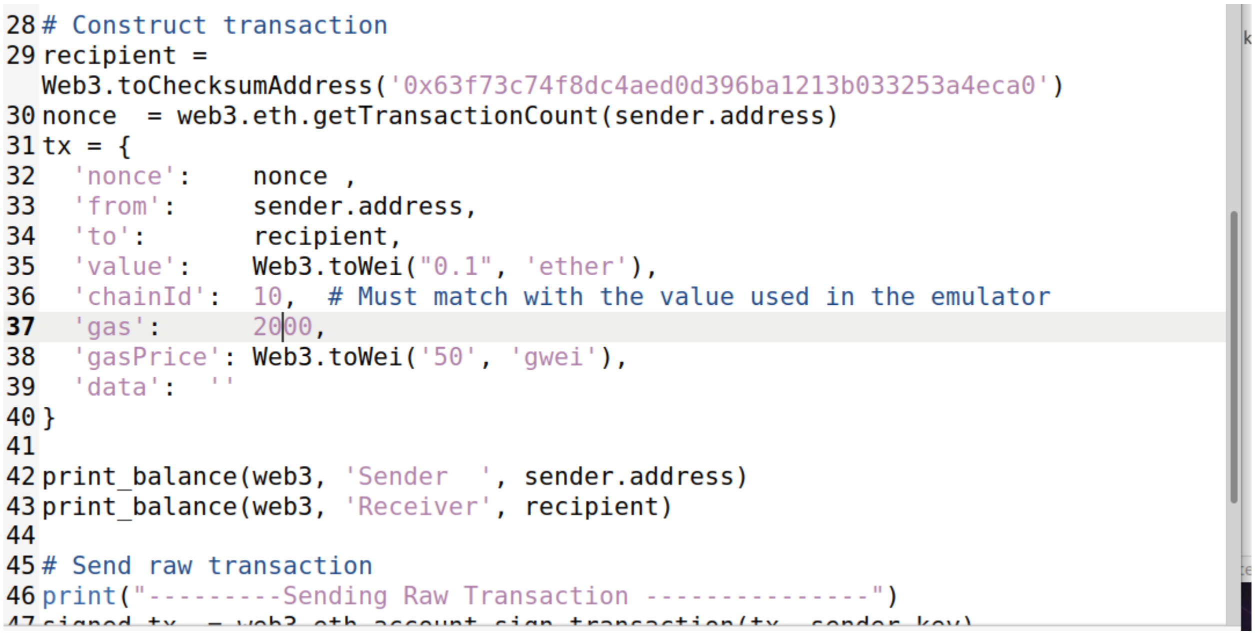
Transaction Details :



```
{
  accessList: [],
  blockHash: "0xb2ac24aee41258a4afcb795b0b90bb8fa36be4b0bc69f1e09618f7abea0f7a98",
  blockNumber: 92,
  chainId: "0xa",
  from: "0xeb2b3ce5b4a2c33497707eb962ec97b190fc9541",
  gas: 21000,
  gasPrice: 1000004630,
  hash: "0xf60906e4a1b6e933efa20fac5bc7111bba97a1a5ed74b826d2aba80da0b74afa",
  input: "0x",
  maxFeePerGas: 1000010582,
  maxPriorityFeePerGas: 1000000000,
  nonce: 1,
  r: "0x85466c282a3992d1b3a6917e82d134b3794b079925d86ab41ee0d9571c00da43",
  s: "0x723a0c141f9d3245ea1065cce8e1a3d2815296d17e2f43c9ea929f841e12c3e3",
  to: "0xc720bcdce1649574d5d3dc48a957da38da09caac",
  transactionIndex: 0,
  type: "0x2",
  v: "0x1",
  value: 77777
}
```

Gas and Nonce Experiments:

Here change the Gas too low and we would see that the transaction gets stuck without completion as we do not have enough and also the gas that is used once is already used and can not be gained back and without completion it would still be on the block and the gas would be paid/used up without it being complete.

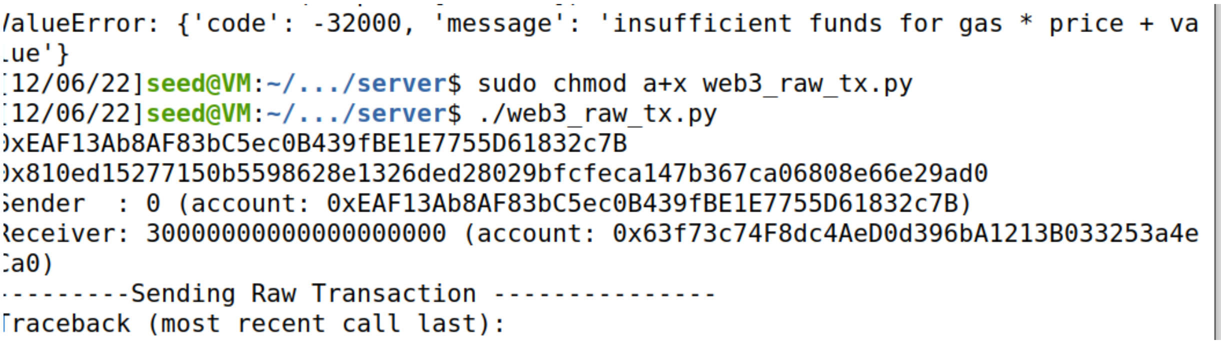


```
# Construct transaction
recipient = 
Web3.toChecksumAddress('0x63f73c74f8dc4aed0d396ba1213b033253a4eca0')
nonce  = web3.eth.getTransactionCount(sender.address)
tx = {
  'nonce':    nonce ,
  'from':     sender.address,
  'to':       recipient,
  'value':    Web3.toWei("0.1", 'ether'),
  'chainId':  10,  # Must match with the value used in the emulator
  'gas':      2000,
  'gasPrice': Web3.toWei('50', 'gwei'),
  'data':  ''
}

print_balance(web3, 'Sender  ', sender.address)
print_balance(web3, 'Receiver', recipient)

# Send raw transaction
print("---------Sending Raw Transaction ---------------")
signed_tx  = web3.eth.account.sign_transaction(tx, sender_key)
```

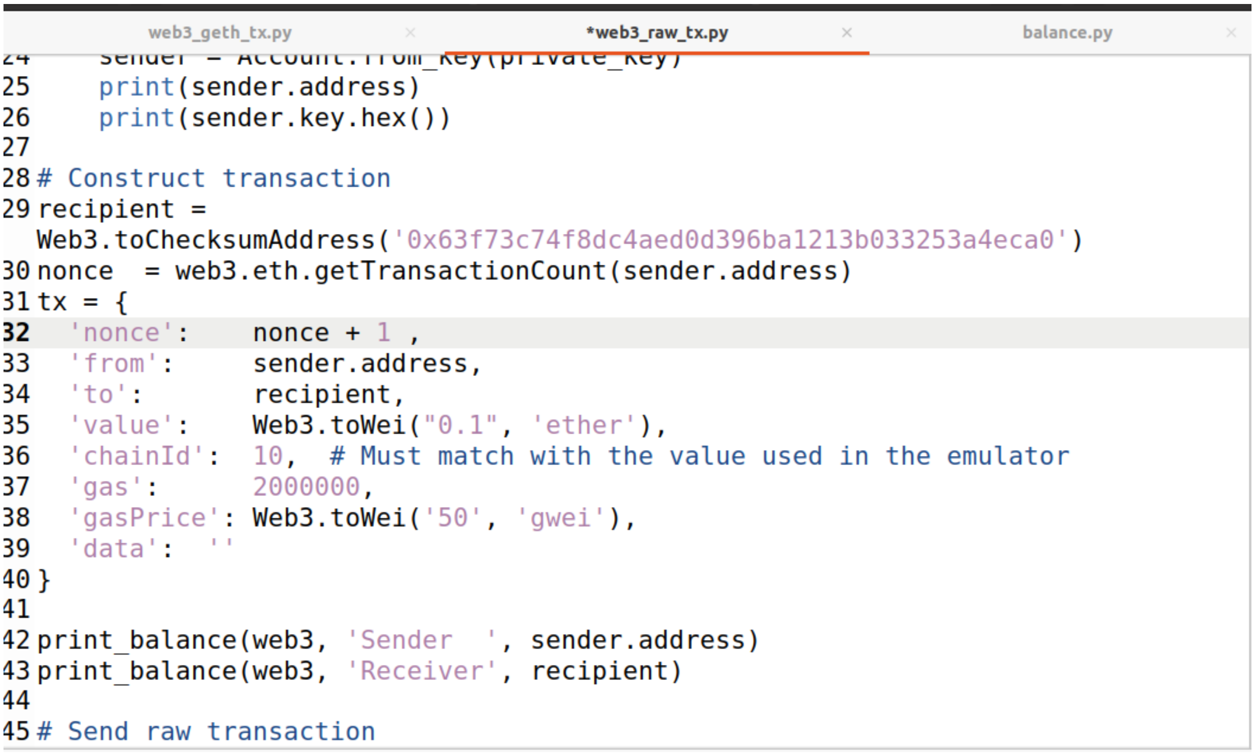
The gas fee is calculated using Gas Limit * Gas Price per Unit. So if the gas limit was 20,000 and the price per unit was 50 gwei, the calculation would be 20,000 * 50 = 1,00,000 gwei.

There can be multiple situations with relation to Gas:

Gas limit can be seen as the gas you are willing to burn for the transaction to complete it may happen that the transaction is not complete, but you have exhausted your limit.
Gas price being low means it can be replaced by a higher gas price to complete transaction or it will be stuck without committing.



```
/alueError: {'code': -32000, 'message': 'insufficient funds for gas * price + va
.ue'}
[12/06/22]seed@VM:~/.../server$ sudo chmod a+x web3_raw_tx.py
[12/06/22]seed@VM:~/.../server$ ./web3_raw_tx.py
)xEAF13Ab8AF83bC5ec0B439fBE1E7755D61832c7B
)x810ed15277150b5598628e1326ded28029bfcfeca147b367ca06808e66e29ad0
;ender   : 0 (account: 0xEAF13Ab8AF83bC5ec0B439fBE1E7755D61832c7B)
{eceiver: 30000000000000000000 (account: 0x63f73c74F8dc4AeD0d396bA1213B033253a4e
:a0)
---------Sending Raw Transaction ---------------
Traceback (most recent call last):
```

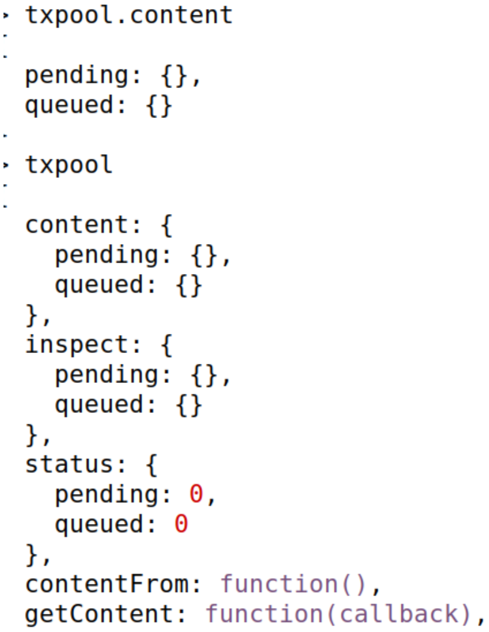


```
    sender = Account.from_key(private_key)
    print(sender.address)
    print(sender.key.hex())

# Construct transaction
recipient = 
 Web3.toChecksumAddress('0x63f73c74f8dc4aed0d396ba1213b033253a4eca0')
nonce   = web3.eth.getTransactionCount(sender.address)
tx = {
  'nonce':     nonce + 1 ,
  'from':      sender.address,
  'to':        recipient,
  'value':     Web3.toWei("0.1", 'ether'),
  'chainId':   10,  # Must match with the value used in the emulator
  'gas':       2000000,
  'gasPrice': Web3.toWei('50', 'gwei'),
  'data':   ''
}

print_balance(web3, 'Sender   ', sender.address)
print_balance(web3, 'Receiver', recipient)

# Send raw transaction
```

In this we make the selection of nonce as current +1, in that case it will get stuck when we send a transaction because there will be a gap between the current nonce state and the consecutive nonce.

If we send another nonce with nonce set to current value then the current transaction as well as the transaction at current + 1 will be executed.

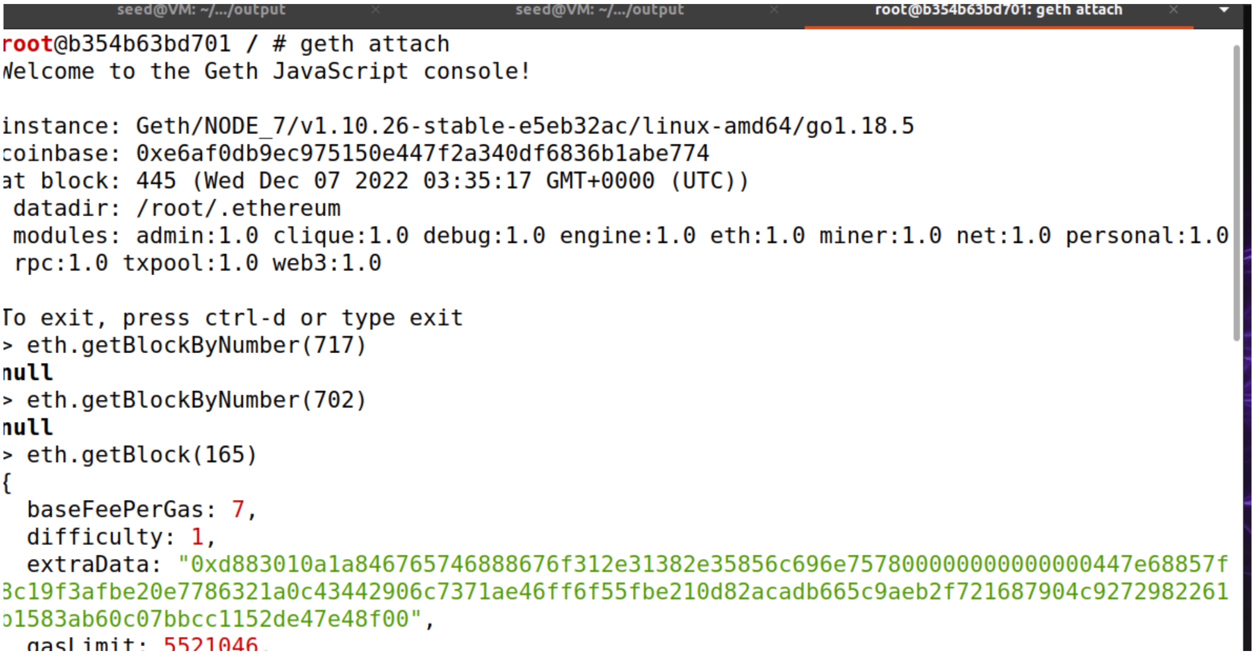
We can then check if that happens the case in txpool (Transaction Pool).content



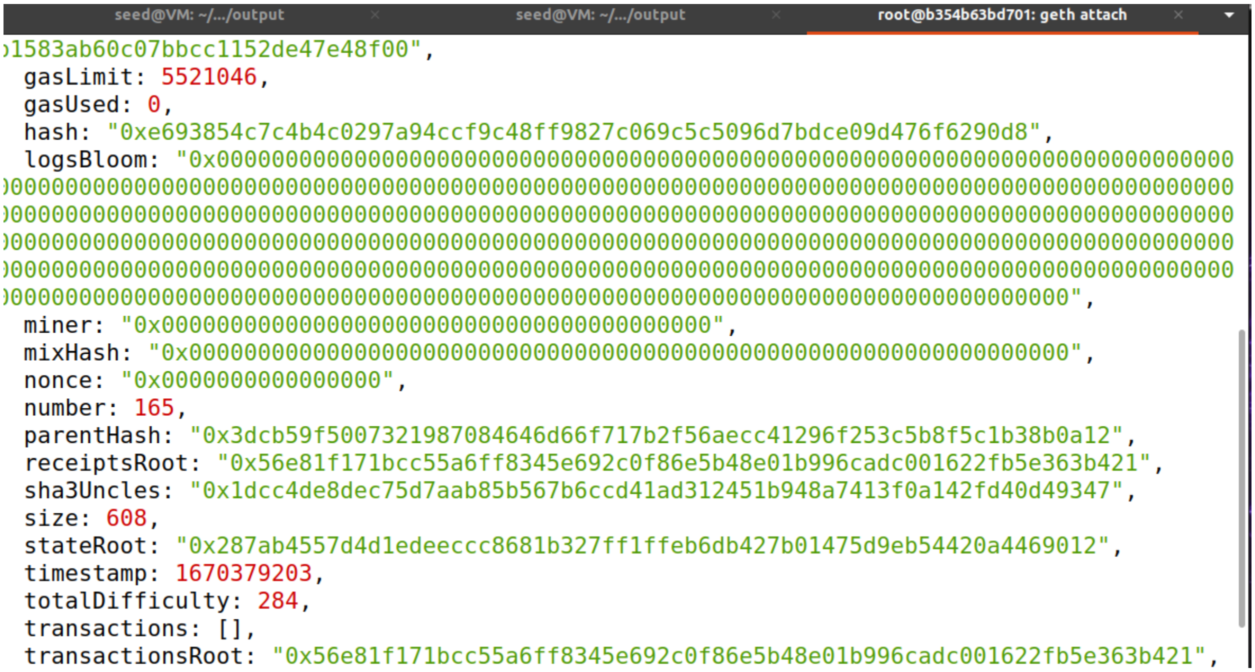
```
> txpool.content

  pending: {},
  queued: {}

> txpool

  content: {
    pending: {},
    queued: {}
  },
  inspect: {
    pending: {},
    queued: {}
  },
  status: {
    pending: 0,
    queued: 0
  },
  contentFrom: function(),
  getContent: function(callback),
```

Tasks with Signer block:

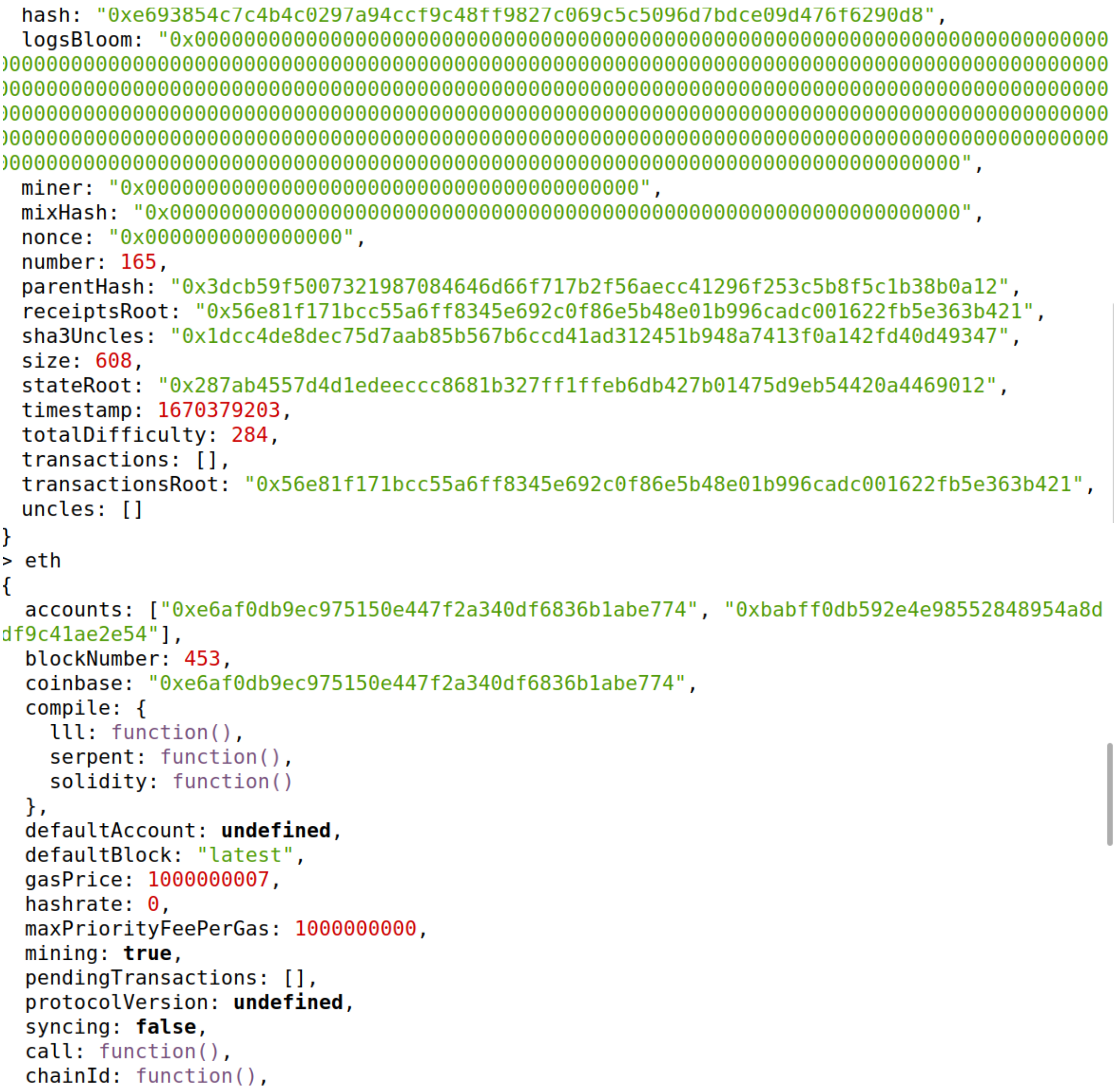
We find a signer node from dockps and get our JScon there:



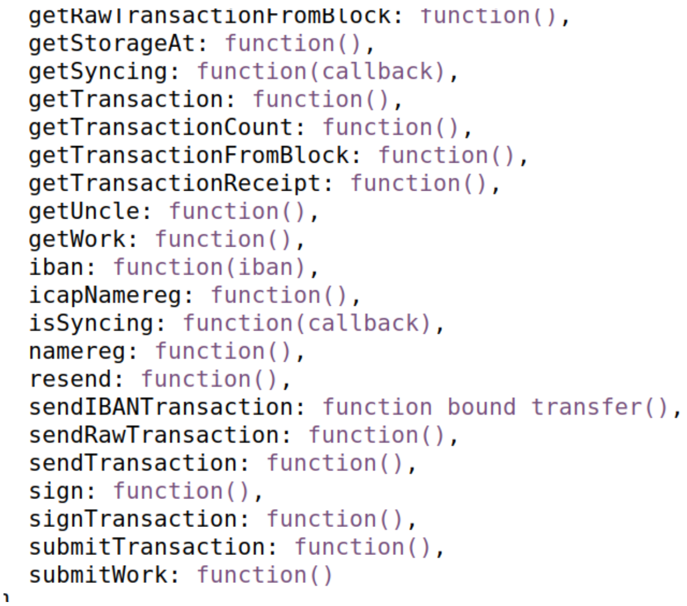
```
root@b354b63bd701 / # geth attach
Welcome to the Geth JavaScript console!

instance: Geth/NODE_7/v1.10.26-stable-e5eb32ac/linux-amd64/go1.18.5
coinbase: 0xe6af0db9ec975150e447f2a340df6836b1abe774
at block: 445 (Wed Dec 07 2022 03:35:17 GMT+0000 (UTC))
 datadir: /root/.ethereum
 modules: admin:1.0 clique:1.0 debug:1.0 engine:1.0 eth:1.0 miner:1.0 net:1.0 personal:1.0
 rpc:1.0 txpool:1.0 web3:1.0

To exit, press ctrl-d or type exit
> eth.getBlockByNumber(717)
null
> eth.getBlockByNumber(702)
null
> eth.getBlock(165)
{
  baseFeePerGas: 7,
  difficulty: 1,
  extraData: "0xd883010a1a846765746888676f312e31382e35856c696e757800000000000000447e68857f
3c19f3afbe20e7786321a0c43442906c7371ae46ff6f55fbe210d82acadb665c9aeb2f721687904c9272982261
b1583ab60c07bbcc1152de47e48f00",
  gasLimit: 5521046,
```



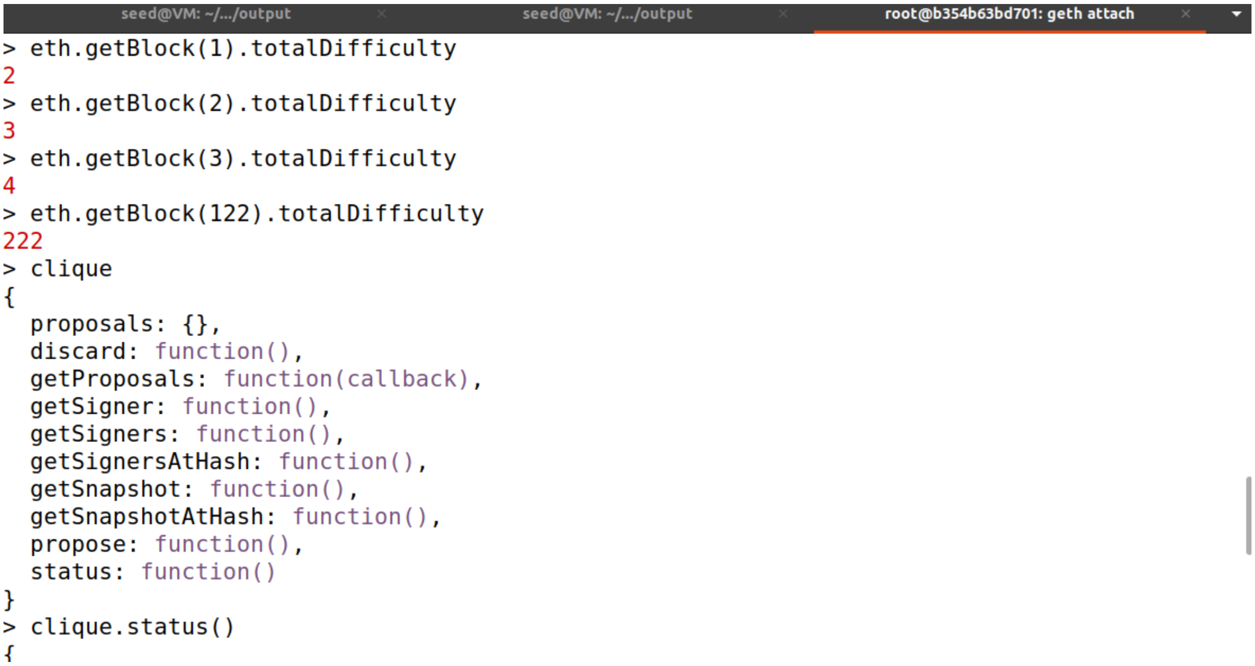
```
b1583ab60c07bbcc1152de47e48f00",
  gasLimit: 5521046,
  gasUsed: 0,
  hash: "0xe693854c7c4b4c0297a94ccf9c48ff9827c069c5c5096d7bdce09d476f6290d8",
  logsBloom: "0x00000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000",
  miner: "0x0000000000000000000000000000000000000000",
  mixHash: "0x0000000000000000000000000000000000000000000000000000000000000000",
  nonce: "0x0000000000000000",
  number: 165,
  parentHash: "0x3dcb59f5007321987084646d66f717b2f56aecc41296f253c5b8f5c1b38b0a12",
  receiptsRoot: "0x56e81f171bcc55a6ff8345e692c0f86e5b48e01b996cadc001622fb5e363b421",
  sha3Uncles: "0x1dcc4de8dec75d7aab85b567b6ccd41ad312451b948a7413f0a142fd40d49347",
  size: 608,
  stateRoot: "0x287ab4557d4d1edeeccc8681b327ff1ffeb6db427b01475d9eb54420a4469012",
  timestamp: 1670379203,
  totalDifficulty: 284,
  transactions: [],
  transactionsRoot: "0x56e81f171bcc55a6ff8345e692c0f86e5b48e01b996cadc001622fb5e363b421",
```



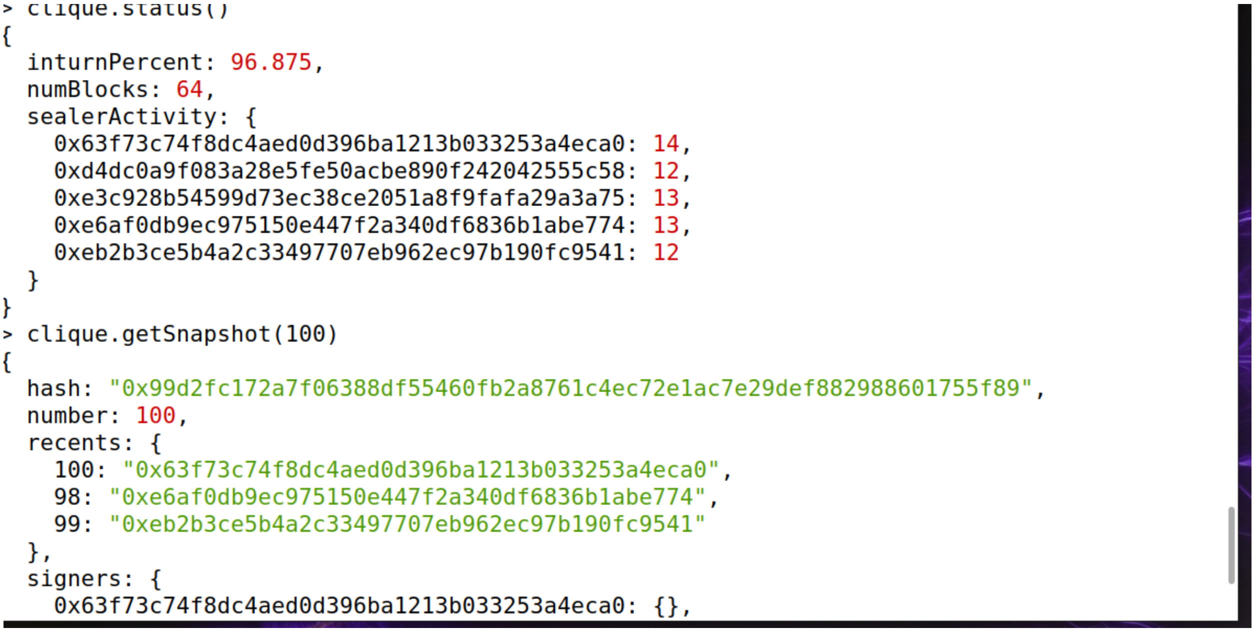
```
  hash: "0xe693854c7c4b4c0297a94ccf9c48ff9827c069c5c5096d7bdce09d476f6290d8",
  logsBloom: "0x00000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000",
  miner: "0x0000000000000000000000000000000000000000",
  mixHash: "0x0000000000000000000000000000000000000000000000000000000000000000",
  nonce: "0x0000000000000000",
  number: 165,
  parentHash: "0x3dcb59f5007321987084646d66f717b2f56aecc41296f253c5b8f5c1b38b0a12",
  receiptsRoot: "0x56e81f171bcc55a6ff8345e692c0f86e5b48e01b996cadc001622fb5e363b421",
  sha3Uncles: "0x1dcc4de8dec75d7aab85b567b6ccd41ad312451b948a7413f0a142fd40d49347",
  size: 608,
  stateRoot: "0x287ab4557d4d1edeeccc8681b327ff1ffeb6db427b01475d9eb54420a4469012",
  timestamp: 1670379203,
  totalDifficulty: 284,
  transactions: [],
  transactionsRoot: "0x56e81f171bcc55a6ff8345e692c0f86e5b48e01b996cadc001622fb5e363b421",
  uncles: []
}
> eth
{
  accounts: ["0xe6af0db9ec975150e447f2a340df6836b1abe774", "0xbabff0db592e4e98552848954a8d
df9c41ae2e54"],
  blockNumber: 453,
  coinbase: "0xe6af0db9ec975150e447f2a340df6836b1abe774",
  compile: {
    lll: function(),
    serpent: function(),
    solidity: function()
  },
  defaultAccount: undefined,
  defaultBlock: "latest",
  gasPrice: 1000000007,
  hashrate: 0,
  maxPriorityFeePerGas: 1000000000,
  mining: true,
  pendingTransactions: [],
  protocolVersion: undefined,
  syncing: false,
  call: function(),
  chainId: function(),
```



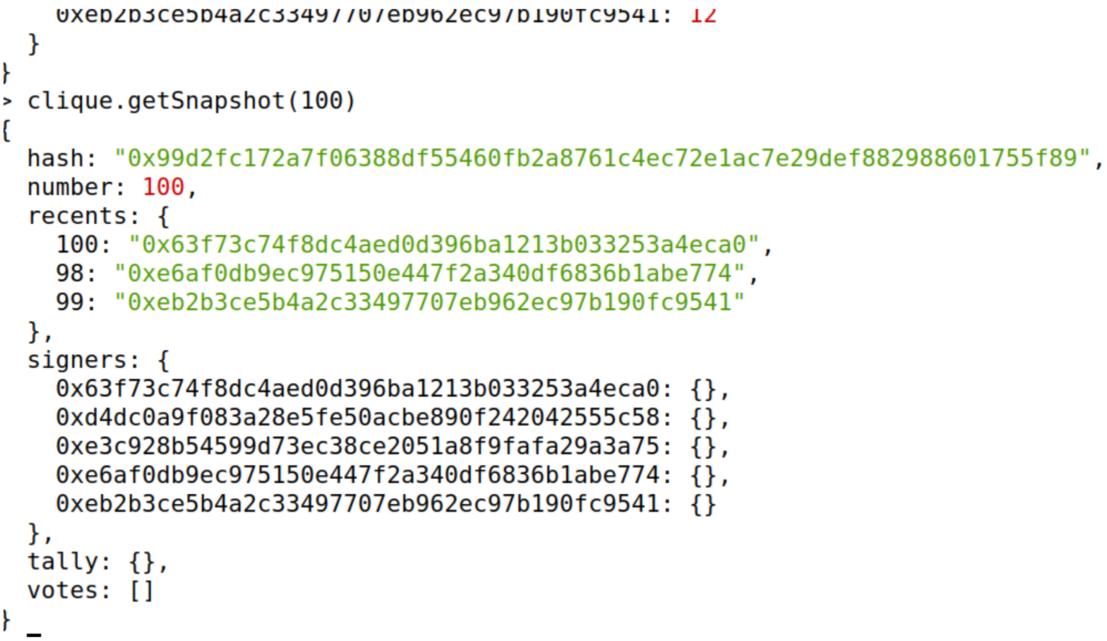
```
  getRawTransactionFromBlock: function(),
  getStorageAt: function(),
  getSyncing: function(callback),
  getTransaction: function(),
  getTransactionCount: function(),
  getTransactionFromBlock: function(),
  getTransactionReceipt: function(),
  getUncle: function(),
  getWork: function(),
  iban: function(iban),
  icapNamereg: function(),
  isSyncing: function(callback),
  namereg: function(),
  resend: function(),
  sendIBANTransaction: function bound transfer(),
  sendRawTransaction: function(),
  sendTransaction: function(),
  sign: function(),
  signTransaction: function(),
  submitTransaction: function(),
  submitWork: function()
}
```



```
> eth.getBlock(1).totalDifficulty
2
> eth.getBlock(2).totalDifficulty
3
> eth.getBlock(3).totalDifficulty
4
> eth.getBlock(122).totalDifficulty
222
> clique
{
  proposals: {},
  discard: function(),
  getProposals: function(callback),
  getSigner: function(),
  getSigners: function(),
  getSignersAtHash: function(),
  getSnapshot: function(),
  getSnapshotAtHash: function(),
  propose: function(),
  status: function()
}
> clique.status()
{
```



```
> clique.status()
{
  inturnPercent: 96.875,
  numBlocks: 64,
  sealerActivity: {
    0x63f73c74f8dc4aed0d396ba1213b033253a4eca0: 14,
    0xd4dc0a9f083a28e5fe50acbe890f242042555c58: 12,
    0xe3c928b54599d73ec38ce2051a8f9fafa29a3a75: 13,
    0xe6af0db9ec975150e447f2a340df6836b1abe774: 13,
    0xeb2b3ce5b4a2c33497707eb962ec97b190fc9541: 12
  }
}
> clique.getSnapshot(100)
{
  hash: "0x99d2fc172a7f06388df55460fb2a8761c4ec72e1ac7e29def882988601755f89",
  number: 100,
  recents: {
    100: "0x63f73c74f8dc4aed0d396ba1213b033253a4eca0",
    98: "0xe6af0db9ec975150e447f2a340df6836b1abe774",
    99: "0xeb2b3ce5b4a2c33497707eb962ec97b190fc9541"
  },
  signers: {
    0x63f73c74f8dc4aed0d396ba1213b033253a4eca0: {},
```



```
    0xeb2b3ce5b4a2c33497707eb962ec97b190fc9541: 12
  }
}
> clique.getSnapshot(100)
{
  hash: "0x99d2fc172a7f06388df55460fb2a8761c4ec72e1ac7e29def882988601755f89",
  number: 100,
  recents: {
    100: "0x63f73c74f8dc4aed0d396ba1213b033253a4eca0",
    98: "0xe6af0db9ec975150e447f2a340df6836b1abe774",
    99: "0xeb2b3ce5b4a2c33497707eb962ec97b190fc9541"
  },
  signers: {
    0x63f73c74f8dc4aed0d396ba1213b033253a4eca0: {},
    0xd4dc0a9f083a28e5fe50acbe890f242042555c58: {},
    0xe3c928b54599d73ec38ce2051a8f9fafa29a3a75: {},
    0xe6af0db9ec975150e447f2a340df6836b1abe774: {},
    0xeb2b3ce5b4a2c33497707eb962ec97b190fc9541: {}
  },
  tally: {},
  votes: []
} _
```