بخش اول: تولید آدرس

```
bitcoin address: n2px8MPScKUkhiWZxckkTHZQVda14g4svz
Private Key (WIF): 92ABWZK4kLxN1EqbkPLQcUntwm5ZfLE4SxR6o8WQSfHSXLjwJZc
```

```
[ ]  def getWif(privkey):
         wif = b"\xef" + privkey # 0xef for testnet and 0x80 for mainnet
         checksum = sha256(sha256(wif).digest()).digest()[:4]
         wif += checksum
         return base58.b58encode(wif)
```

```
prependNetworkByte = '6f' + ridemp160FromHash256.hex() # 0x6f for testnet and 0x00 for mainnet
# print("Prepend Network Byte to RIDEMP160(SHA256(ECDSA Public Key)): ", prependNetworkByte)

hash = prependNetworkByte
for x in range(1,3):
    hash = sha256(binascii.unhexlify(hash)).hexdigest()
    # print("\t|___>SHA256 #", x, " : ", hash)
```

.1

فرق آدرس های شبکه اصلی بیت کوین و شبکه تست در بایت اول آنها است و (همچنین چک سام). در مورد کلید خصوصی به فرمت ویف برای شبکه تست یک بایت (0xef) اضافه می کنیم به اول کلید خصوصی و برای شبکه اصلی یک بایت (0x80) اضافه می کنیم و سپس انکد می کنیم. در مورد آدرس نیز در شبکه تست یک بایت (0x6f) به اول هش کلید عمومی اضافه می کنیم و در شبکه اصلی بایت (0x00) اضافه می کنیم و سپس انکد می کنیم.

آدرس‌های شبکه اصلی با 1، 3 یا bc1 شروع می‌شوند، در حالی که آدرس‌های شبکه آزمایشی با 2، m، n یا tb1 شروع می‌شوند.

.2

```
desired_prefix = "pik"
vanity_address, vanity_wif = find_vanity_address(desired_prefix)
print(f"Vanity Address: {vanity_address.decode()}")
print(f"Private Key (WIF): {vanity_wif.decode()}")
```

```
Vanity Address: mpikALrCM4VDR6gmd3K7638pGQALyd32xK
Private Key (WIF): 92ccUJ7FUaw7vPUKfXTmBF5k1DBJ77GWify7N9sEQuTxunsKcHk
```

بخش اول: ایجاد تراکنش

همه تراکنش ها در شبکه تست نت 4 انجام شده است و در آدرس زیر قابل مشاهده است:

https://mempool.space/testnet4

تراکنش یک:

My address = **mm2DuQFF87QZcA4Fx91hYZhMJ4Q5ksZqsy**

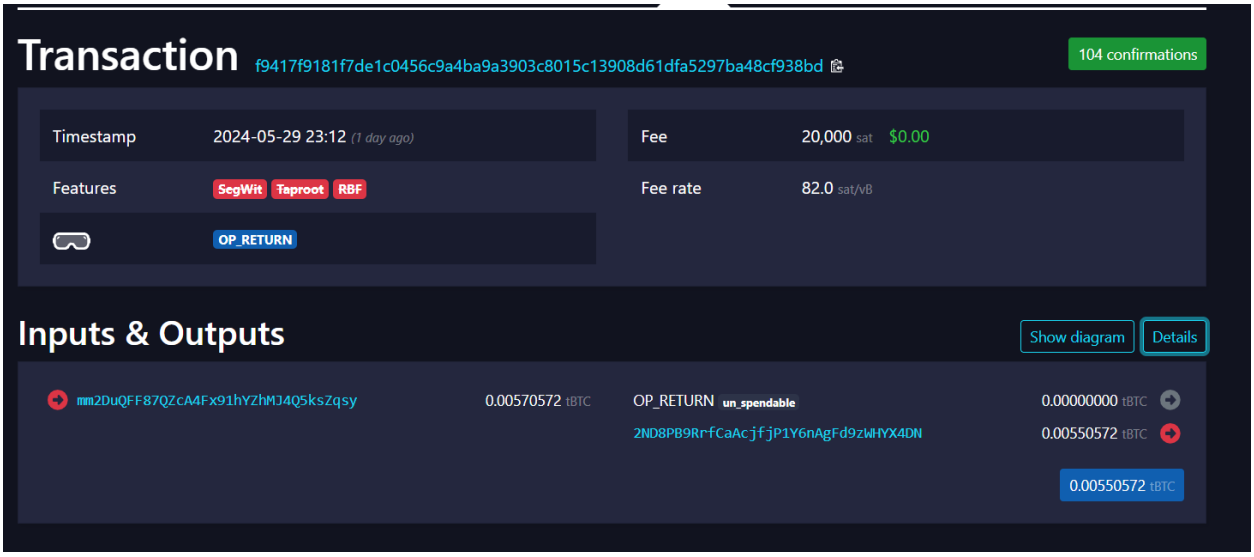
My seckey (WIF) = **91uYe7oEQaeQUMtDxHrzLqQfpa82hKtxutF5p3Uf9TDGBsArcjL**

faucet txid = **ff5ad8d5b0cd7b0489efe84ce018b4f2529559f6b3d0fb1e378b718d835d0821**

first transaction: **f9417f9181f7de1c0456c9a4ba9a3903c8015c13908d61dfa5297ba48cf938bd**

spend transaction: **de261c3f93e08fffffb6cf3ac3d6cc562df71cfe6a932ac3e561bc820165c7f2**

تراکنش رفت:



تراکنش برگشت:

تراکنش دو:

my_address = **mtc38q1o1ECwz5LP3MEERx3BZwAkSiDcKH**

my_seckey = **92yyk3sjqzTTXoTAk9XcHPvxB3pFdiLGF5bDzZTr7GJUSwGCEQC**

faucet txid =
ff5ad8d5b0cd7b0489efe84ce018b4f2529559f6b3d0fb1e378b718d835d0821

address1 = **n18umQTMWjWJ3wALS4UfLmAByQ2N3gijU7**

seckey1 = **93N2Hw71bHAcvkn4JM3VLqW8e3MYJRyoDVe5aXdbvmh7XCX5Fyz**

address2 = **mpD8ZgnA2e9WZkKGXRXboU1ABmGxgCuaa9**

seckey2 = **93Q5PZFgZfM9EcuDHf5Q8ASrv4K53QNWMkiVPFPtJmUQA6pWK5s**

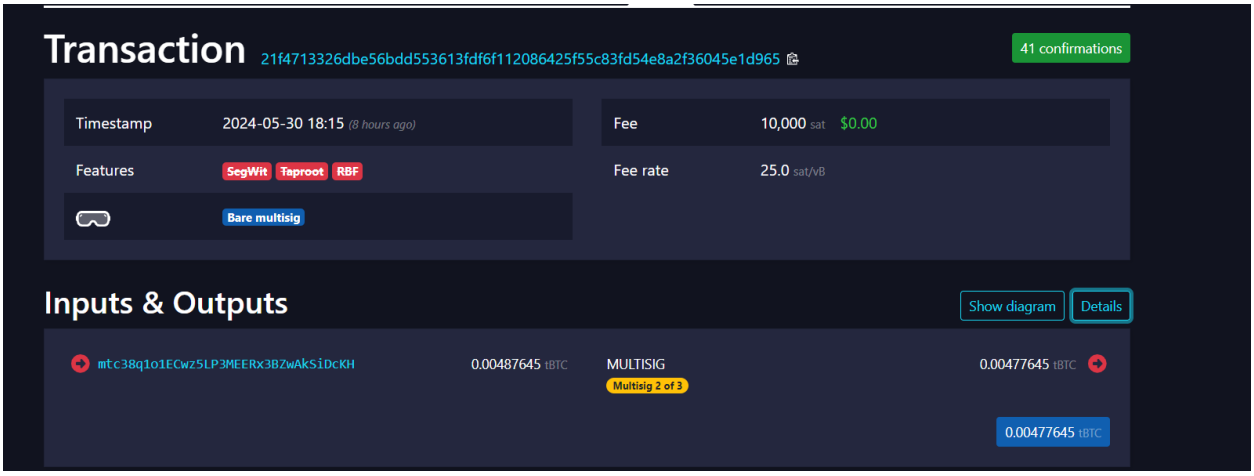
address3 = **n2px8MPScKUkhiWZxckkTHZQVda14g4svz**

seckey3 = **92ABWZK4kLxN1EqbkPLQcUntwm5ZfLE4SxR6o8WQSfHSXLjwJZc**

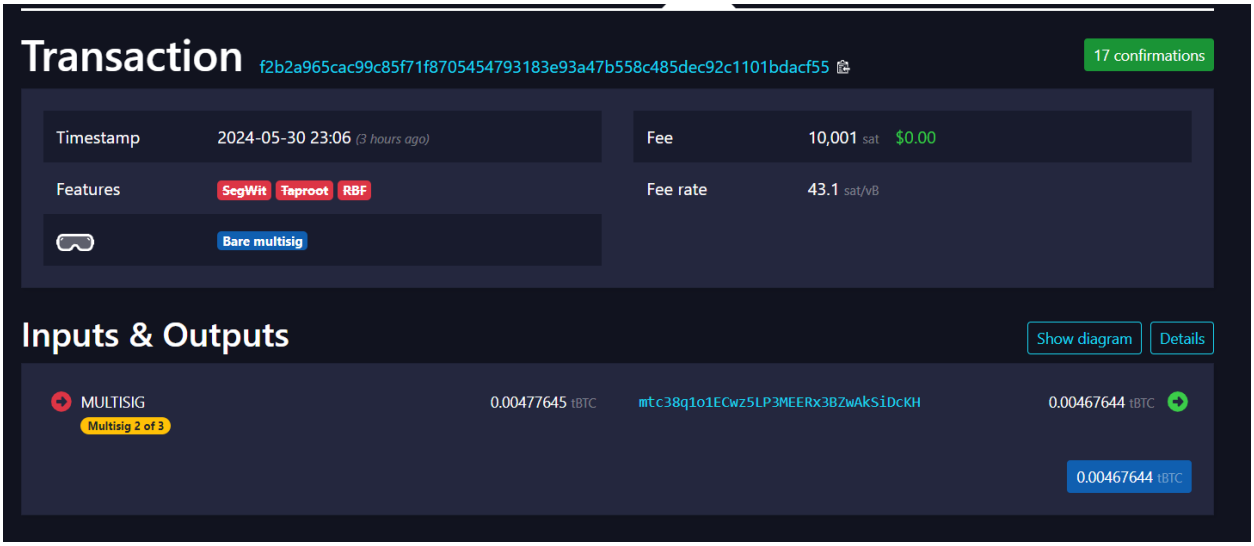
first transaction:
21f4713326dbe56bdd553613fdf6f112086425f55c83fd54e8a2f36045e1d965

back transaction:
f2b2a965cac99c85f71f8705454793183e93a47b558c485dec92c1101bdacf55

تراکنش رفت:



تراکنش برگشت:



تراکنش سه:

Redeem script:

```
return [OP_IF,
            current_year, OP_SWAP, OP_SUB, legal_age, OP_GREATERTHAN, OP_VERIFY,
        OP_ELSE,
            OP_SHA256, hashed_password, OP_EQUALVERIFY,
        OP_ENDIF,
        public_key, OP_CHECKSIG
    ]
```

Lock script:

```
return [OP_HASH160, Hash160(CScript(redeem_script)), OP_EQUAL]
```

---------- BY_BIRTH_YEAR ----------

Unlock script:

```
unlock_script = [sig, birth_year, OP_TRUE, CScript(redeem_script)]
```

My address **= mm9c8NT3wVQvdhdcwUdBSJYD5RC3QWfDLF**

My seckey **= 92RAXdXFEykJsrCqaBjPhbetFYNgQdpeena3oncxXP8MVFGhQzn**

faucet **txid = 6efc4bbadf7574e54ec9b9abf9d6ff103675050fa11c7e9c82966db88cf05990**

dst_address = **mm9c8NT3wVQvdhdcwUdBSJYD5RC3QWfDLF**

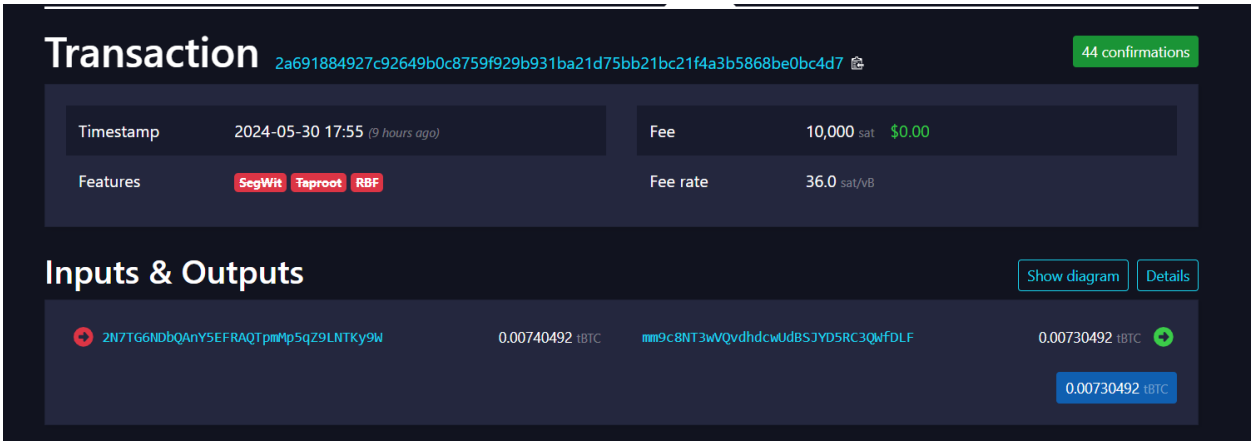
dst_seckey = **92RAXdXFEykJsrCqaBjPhbetFYNgQdpeena3oncxXP8MVFGhQzn**

first transaction **=**
f0c813582d132e1e235aec1f1f905fbc0e1cf504a71ae887caeac8a274982443

spend by birth year **=**
2a691884927c92649b0c8759f929b931ba21d75bb21bc21f4a3b5868be0bc4d7

تراکنش رفت:

تراکنش خرج کردن با بررسی سال تولد:



```
P2SH redeem script      OP_IF
                        OP_PUSHBYTES_2 e807
                        OP_SWAP
                        OP_SUB
                        OP_PUSHBYTES_1 12
                        OP_GREATERTHAN
                        OP_VERIFY
                        OP_ELSE
                        OP_SHA256
                        OP_PUSHBYTES_32 6009b3c19a19f84e6b5208493a41193
                        9d0f49a90b462aa55b5b32466602c80b4
                        OP_EQUALVERIFY
                        OP_ENDIF
                        OP_PUSHBYTES_65 04b7327478cf2c4d82a3d7dc3cfeb34
                        d157dfccc0dc07d3520956266b1bb001c21668496e96dc1
                        49eef05de8eead82c6a1c3cd42aabbf27910d247d699e30
                        0a494
                        OP_CHECKSIG
```

---------- BY_PASSWORD----------

Unlock script:

```
txin_scriptSig = [sig, password, OP_FALSE, CScript(redeem_script)]
```

My address = **mpfae6CyUZKVjNirUjKufQQqnYyY8eyCEq**

My seckey = **92iTTc78XusdQ3FwwoF6Ey4pinhyjiddHKiWNzPzSvjvMHqPij4**

faucet txid = **34370a255f3c56e392933ba666301145020847482db6931e6fa9934e46978182**

dst_address = **mhCnXhJT4jtH5naGr3nx2ZwSboECLuVTqB**

dst_seckey = **928u9S4ztkQiS6oeZBtryU46HjeCjFwPULGcmKEoKUpwD1wiwhq**

first transaction =
52ceb80c5c7a5a0eb6bd2fe84de9aaf119b6339e74648e300c3175ae0174c7d5

spend by password =
d1a68c8f20cc0ce8297e4f4b5ec297af1c6f98630e8105fd9d63b39c004c4ff0

تراکنش رفت:

Transaction 52ceb80c5c7a5a0eb6bd2fe84de9aaf119b6339e74648e300c3175ae0174c7d5 — 59 confirmations

Timestamp	2024-05-30 13:22 *(13 hours ago)*	Fee	10,001 sat $0.00
Features	SegWit Taproot RBF	Fee rate	45.3 sat/vB

Inputs & Outputs — Show diagram | Details

mpfae6CyUZKVjNirUjKufQQqnYyY8eyCEq	0.00499172 tBTC	2NCheodrwBXojK6sQzKh7BsY8Gnmz4e7fze	0.00489171 tBTC
			0.00489171 tBTC

mpfae6CyUZKVjNirUjKufQQqnYyY8eyCEq — 0.00499172 tBTC

ScriptSig (ASM)
```
OP_PUSHBYTES_71 304402205e62323d3827d5ac7ef0abb
7c19716b559491d3977d1fc5d495af7d3b0dd2676022055
c7054e2ffeaf69a88a0670cc03af9cffc3d1ce24cb13e35
107c7f0ebb0384501
OP_PUSHBYTES_65 04805c4604fce84fe40006a9567f23e
77290eb80dff8b0126d2a8d97f9efcc3dbbe9a4e52a228e
1b8fc6564bde631d97b97ef864b101bc9f9f926e83d9246
c5b8d
```

2NCheodrwBXojK6sQzKh7BsY8Gnmz4e7fze — 0.00489171 tBTC

ScriptPubKey (ASM)
```
OP_HASH160
OP_PUSHBYTES_20 d569ebaca3b27115a284275caae0359
4e3e50db6
OP_EQUAL
```

ScriptPubKey (HEX) a914d569ebaca3b27115a284275caae03594e3e50db687

Type P2SH

تراکنش خرج کردن با پسورد:

Transaction d1a68c8f20cc0ce8297e4f4b5ec297af1c6f98630e8105fd9d63b39c004c4ff0 — 52 confirmations

Timestamp	2024-05-30 15:47 *(11 hours ago)*	Fee	10,001 sat $0.00
Features	SegWit Taproot RBF	Fee rate	35.2 sat/vB

Inputs & Outputs — Show diagram | Details

2NCheodrwBXojK6sQzKh7BsY8Gnmz4e7fze	0.00489171 tBTC	mpfae6CyUZKVjNirUjKufQQqnYyY8eyCEq	0.00479170 tBTC
			0.00479170 tBTC

```
P2SH redeem script        OP_IF
                          OP_PUSHBYTES_2 2024
                          OP_SWAP
                          OP_SUB
                          OP_PUSHBYTES_1 18
                          OP_GREATERTHAN
                          OP_VERIFY
                          OP_ELSE
                          OP_SHA256
                          OP_PUSHBYTES_32 6009b3c19a19f84e6b5208493a41193
                          9d0f49a90b462aa55b5b32466602c80b4
                          OP_EQUALVERIFY
                          OP_ENDIF
                          OP_PUSHBYTES_65 0443a74996f06a600889469f3f98234
                          5d7ce7e55081713daaaba42c317f18897d6ad9f0246eed4
                          d0a9a3d684330df0aa0c3fde697de7312315244123cc230
                          9eb74
                          OP_CHECKSIG
```

```
# Create scriptSig
txin_scriptSig = [sig, password, OP_FALSE, CScript(redeem_script)]
```

.1

کاهش رمزارزهای در گردش

یکی از مزایای الگوریتم اثبات سوزاندن، کاهش رمزارزهای در گردش است. به دلیل اینکه نودهای شبکه برای ایجاد بلاک‌های جدید مجبور به سوزاندن کوین‌های شبکه هستند، همواره عرضه آن‌ها کم شده و در نتیجه قیمت آن افزایش می‌یابد.

ایمنی شبکه

یکی دیگر از مزایای مکانیسم اثبات سوزاندن، ایمن بودن این مکانیسم است؛ زیرا همچون روشPoW ، استخراج‌کنندگان تمام تلاش خود را می‌کنند تا شبکه به درستی کار کند و از هدر رفتن سرمایه‌هایشان جلوگیری شود. در روش PoB نیز ماینرها توکن‌های خود را می‌سوزانند و تلاش می‌کنند شبکه به درستی کار کند، تا بلاک بعدی ایجاد شود و آن‌ها پاداششان را دریافت کنند. در این روش مانندPoW ، ماینرها در ازای سوزاندن کوین‌های خود انتظار دارند تا پس از مدتی با ایجاد بلاک‌های جدید و دریافت پاداش، سپرده‌گذاری اولیه خود را دریافت کنند و به سود برسند .

سوزاندن کوین‌ها و عدم بازگشت آن‌ها به شبکه

یکی از مزایای روش اجماع اثبات سوزاندن نسبت به PoS این است که، در روش اجماع گواه اثبات سهام اعتبارسنج‌ها پس از مدتی به توکن‌های خود دسترسی پیدا می‌کنند و می‌توانند آن‌ها را در بازار به فروش برسانند. این مساله باعث افزایش عرضه کوین‌ها و در نتیجه کاهش قیمت آن‌ها می‌شود؛ اما در الگوریتم گواه اثبات سوزاندن، اعتبارسنج‌ها دیگر به کوین‌های خود دسترسی نداشته و روند عرضه کوین‌ها دائما در حال کاهش است. این مساله می‌تواند به ارزشمند شدن و افزایش بهای کوین شبکه‌هایی که از POB بهره می‌برند، کمک شایانی داشته باشد.

مزایای اقتصادی در الگوریتم اثبات سوزاندن

الگوریتم Proof Of Burn دارای ویژگی‌های اقتصادی است که آن را از Pow و PoS متمایز می‌کند. در روش اجماع اثبات سوزاندن به علت سوزانده شدن کوین‌ها برای ایجاد بلاک جدید تعداد کوین‌های در گردش کنترل شود. این مساله باعث می‌شود کارایی الگوریتم Proof Of Burn نسبت به دو روش دیگر از مزایای اقتصادی بیشتری بهره‌مند باشد.

.2

اسکریپت بیت کوین تورینگ کامل نیست. یعنی نمی تواند توابع پیچیده را محاسبه کند زیرا از حلقه ها پشتیبانی نمی کند. اما مزیتی که دارد این است که مشکل حلقه بی نهایت را دیگر ندارد. مزیت یک زبان تورینگ کامل این است ما را قادر می سازد تا توابع پیچیده تری بسازیم.

بخش دوم:

Install geth and getting ready:

```
curl -O
https://gethstore.blob.core.windows.net/builds/geth-
linux-amd64-1.8.10-eae63c51.tar.gz
tar -zxf geth-linux-amd64-1.8.10-eae63c51.tar.gz
sudo ln -s /PATH/TO/DIRECTORY/geth-linux-amd64-1.8.10-
eae63c51/geth /usr/bin/geth
```

```
geth --help
```

```
morteza@Rashidkhan:~$ geth --help
NAME:
   geth - the go-ethereum command line interface

USAGE:
   geth [global options] command [command options] [arguments...]

VERSION:
   1.14.3-stable-ab48ba42

COMMANDS:
   account                 Manage accounts
   attach                  Start an interactive JavaScript environment (connect t
o node)
   console                 Start an interactive JavaScript environment
   db                      Low level database operations
   dump                    Dump a specific block from storage
   dumpconfig              Export configuration values in a TOML format
   dumpgenesis             Dumps genesis block JSON configuration to stdout
   export                  Export blockchain into file
   export-history          Export blockchain history to Era archives
   import                  Import a blockchain file
   import-history          Import an Era archive
   import-preimages        Import the preimage database from an RLP stream
   init                    Bootstrap and initialize a new genesis block
   js                      (DEPRECATED) Execute the specified JavaScript files
   license                 Display license information
   removedb                Remove blockchain and state databases
   show-deprecated-flags   Show flags that have been deprecated
   snapshot                A set of commands based on the snapshot
   verkle                  A set of experimental verkle tree management commands
   version                 Print version numbers
   version-check           Checks (online) for known Geth security vulnerabilitie
s
   wallet                  Manage Ethereum presale wallets
   help, h                 Shows a list of commands or help for one command

GLOBAL OPTIONS:
   ACCOUNT
```

```
account            Manage accounts

attach             Start an interactive JavaScrit
              environment(connect to node)

console            Start an interactive JavaScript
         environment

db                 Low level database operations

dump               Dump a specific block from storage

dumpconfig         Export configuration values in a TOML
              format
```

```
dumpgenesis      Dumps genesis block JSON configuration
             to stdout
export           Export blockchain into file
exportpreimages  Export the preimage database into an
                 RLP stream
import           Import a blockchain file
importpreimages  Import the preimage database from an
                 RLP stream
init             Bootstrap and initialize a new genesis
        block
license          Display license information
removedb         Remove blockchain and state databases
showdeprecatedflags  Show flags that have been
                     deprecated
snapshot         A set of commands based on the
snapshot
verkle           A set of experimental verkle tree
        management commands
version          Print version numbers
versioncheck     Checks (online) for known Geth
                 security vulnerabilities
wallet           Manage Ethereum presale wallets
```

account	**مدیریت حساب ها**
attach	**شروع یک محیط تعاملی جاوا اسکریپت (یا همان متصل شدن به نود)**
console	**شروع یک محیط تعاملی جاوا اسکریپت**
db	**عملیات سطح پایین پایگاه داده**

dump	خروجی گرفتن از ی ک بلوک خاص از ذخی ره سازی
dumpconfig	صادر کردن مقادی ر پ ی کربندی در ی ک فرمتTOML
dumpgenesis	صادر کردن پیکربندی بلوک آغازین به صورت JSON به stdout
export	صادر کردن زنجیره بلوکی به فایل
exportpreimages	صادر کردن پایگاه داده پیش تصاویر به یک جریان RLP
Import	وارد کردن یک فایل زنجیره بلوکی
Importpreimages	وارد کردن پایگاه داده پیش تصاویر از یک جریان RLP
init	بوت استرپ و مقدماتی کردن یک بلوک آغازین جدید
license	نمایش اطالعات مجوز
removedb	حذف پای گاه دادههای زنجیره بلوکی و نشان دهنده وضعیت

Make genesis.json file and nodes:

```
morteza@Rashidkhan:~/Desktop/My_PC/Crypto/CA2$ vim genesis.json
morteza@Rashidkhan:~/Desktop/My_PC/Crypto/CA2$  mkdir node01 node02 node03
morteza@Rashidkhan:~/Desktop/My_PC/Crypto/CA2$ ls
genesis.json  node01  node02  node03
```

```
geth --datadir node01 account new
geth --datadir node02 account new
geth --datadir node03 account new
```

```
morteza@Rashidkhan:~/Desktop/My_PC/Crypto/CA2$  geth --datadir "node01/" account
 new
INFO [05-21|15:20:08.954] Maximum peer count                       ETH=50 total=
50
INFO [05-21|15:20:08.955] Smartcard socket not found, disabling    err="stat /ru
n/pcscd/pcscd.comm: no such file or directory"
Your new account is locked with a password. Please give a password. Do not forge
t this password.
Password:
Repeat password:

Your new key was generated

Public address of the key:   0x49eC6f0a15204f4e0A80CEE29006B3Cf2f88Bcf1
```

توجه: عکس بالا کمی قدیمی است و به همین علت آدرس عمومی آن با چیزی که در genesis است فرق دارد.

Genesis.json:

```
{
"config": {
                "chainId": 15,
                "homesteadBlock": 0,
                "daoForkSupport": true,
                "eip150Block": 0,
                "eip155Block": 0,
                "eip158Block": 0,
                "terminalTotalDifficultyPassed": true
        },
        "difficulty": "400000",
        "gasLimit": "2100000",
        "alloc": {
                "3833f34f72c9d44cd135c3e0ea907afd484c50eb": { "balance": "1000000000810899055" },
                "5c9629152ac81acff5d49a87d0ab5104c9b09e79": { "balance": "2000000000810899055" },
                "fa1eda41af21ee951fe4253bfffab304221dcdf3": { "balance": "1500000000810899055" }
        }
}
~
```

```
geth --datadir node01 init genesis.json
geth --datadir node02 init genesis.json
geth --datadir node03 init genesis.json
```

```
morteza@Rashidkhan:~/Desktop/My_PC/Crypto/CA2$ geth --datadir node01 init genesis.json
INFO [05-31|04:02:33] Maximum peer count                       ETH=25 LES=0 total=25
INFO [05-31|04:02:33] Allocated cache and file handles         database=/home/morteza/Desktop/My_PC/Crypt
o/CA2/node01/geth/chaindata cache=16 handles=16
INFO [05-31|04:02:33] Persisted trie from memory database      nodes=4 size=744.00B time=9.377µs gcnodes=
0 gcsize=0.00B gctime=0s livenodes=1 livesize=0.00B
INFO [05-31|04:02:33] Successfully wrote genesis state         database=chaindata
                                 hash=3fab26…e4272b
INFO [05-31|04:02:33] Allocated cache and file handles         database=/home/morteza/Desktop/My_PC/Crypt
o/CA2/node01/geth/lightchaindata cache=16 handles=16
INFO [05-31|04:02:34] Persisted trie from memory database      nodes=4 size=744.00B time=10.037µs gcnodes
=0 gcsize=0.00B gctime=0s livenodes=1 livesize=0.00B
INFO [05-31|04:02:34] Successfully wrote genesis state         database=lightchaindata
                                 hash=3fab26…e4272b
```

In terminal 1:

```
geth --identity "n1" --rpc --rpcport "8001" --
rpccorsdomain "*" --datadir "node01" --port "30301" --
nodiscover --rpcapi
"db,eth,net,web3,personal,miner,admin" --networkid 1900
--nat "any"
```

In terminal 2:

```
geth --identity "n2" --rpc --rpcport "8002" --
rpccorsdomain "*" --datadir "node02" --port "30302" --
nodiscover --rpcapi
"db,eth,net,web3,personal,miner,admin" --networkid 1900
--nat "any"
```

In terminal 3:

```
geth --identity "n3" --rpc --rpcport "8003" --
rpccorsdomain "*" --datadir "node03" --port "30303" --
nodiscover --rpcapi
"db,eth,net,web3,personal,miner,admin" --networkid 1900
--nat "any"
```

```
morteza@Rashidkhan:~/Desktop/My_PC/Crypto/CA2$ geth --identity "n1" --rpc --rpcport "8001" --rpccorsdomain "*" --datadir "node01" --port "30301" --
nodiscover --rpcapi "db,eth,net,web3,personal,miner,admin" --networkid 1900 --nat "any"
INFO [05-31|04:04:35] Maximum peer count                       ETH=25 LES=0 total=25
INFO [05-31|04:04:35] Starting peer-to-peer node               instance=Geth/n1/v1.8.10-stable-eae63c51/linux-amd64/go1.10.1
INFO [05-31|04:04:35] Allocated cache and file handles         database=/home/morteza/Desktop/My_PC/Crypto/CA2/node01/geth/chaindata cache=768 hand
les=512
INFO [05-31|04:04:35] Initialised chain configuration          config="{ChainID: 15 Homestead: 0 DAO: <nil> DAOSupport: true EIP150: 0 EIP155: 0 EI
P158: 0 Byzantium: <nil> Constantinople: <nil> Engine: unknown}"
INFO [05-31|04:04:35] Disk storage enabled for ethash caches   dir=/home/morteza/Desktop/My_PC/Crypto/CA2/node01/geth/ethash count=3
INFO [05-31|04:04:35] Disk storage enabled for ethash DAGs     dir=/home/morteza/.ethash                                     count=2
INFO [05-31|04:04:35] Initialising Ethereum protocol           versions="[63 62]" network=1900
INFO [05-31|04:04:35] Loaded most recent local header          number=120 hash=b87196…1f6af6 td=47373595
INFO [05-31|04:04:35] Loaded most recent local full block      number=120 hash=b87196…1f6af6 td=47373595
INFO [05-31|04:04:35] Loaded most recent local fast block      number=120 hash=b87196…1f6af6 td=47373595
INFO [05-31|04:04:35] Loaded local transaction journal         transactions=0 dropped=0
INFO [05-31|04:04:35] Regenerated local transaction journal    transactions=0 accounts=0
WARN [05-31|04:04:35] Blockchain not empty, fast sync disabled
INFO [05-31|04:04:35] Starting P2P networking
INFO [05-31|04:04:35] RLPx listener up                         self="enode://9efcdc57d51fe3f5090fd8132b6ec218f8c5f90304aea358508a61c532a3e75a433838
ea489e54a017f63d647cd13fd4d27d10ad3afdfd21a3247511dd306c91@[::]:30301?discport=0"
INFO [05-31|04:04:35] IPC endpoint opened                      url=/home/morteza/Desktop/My_PC/Crypto/CA2/node01/geth.ipc
INFO [05-31|04:04:35] HTTP endpoint opened                     url=http://127.0.0.1:8001                                  cors=* vhosts=localhost
^CINFO [05-31|04:04:39] Got interrupt, shutting down...
INFO [05-31|04:04:39] HTTP endpoint closed                     url=http://127.0.0.1:8001
```

In terminal 4:

```
geth attach http://127.0.0.1:8001
```

```
morteza@Rashidkhan:~/Desktop/My_PC/Crypto/CA2$ geth attach http://127.0.0.1:8001
WARN [05-21|18:06:26.534] Enabling deprecated personal namespace
Welcome to the Geth JavaScript console!

instance: Geth/n1/v1.14.3-stable-ab48ba42/linux-amd64/go1.22.3
at block: 0 (Thu Jan 01 1970 03:30:00 GMT+0330 (+0330))
 datadir: /home/morteza/Desktop/My_PC/Crypto/CA2/node01
 modules: admin:1.0 debug:1.0 eth:1.0 miner:1.0 net:1.0 personal:1.0 rpc:1.0 web3:1.0

To exit, press ctrl-d or type exit
>
```

In terminal 5:

```
geth attach http://127.0.0.1:8002
```

In terminal 6:

```
geth attach http://127.0.0.1:8003
```

In teminal 4:

```
admin.nodeInfo
```

```
> admin.nodeInfo
{
  enode: "enode://433960332a7cd02a0e1158bbd995905c5609c495a4aee44bdcac86649207d4137fc23245d9676202900abc0ff5e007c2c202a35e71e36472ecf82b18367c5f870127.0.0.1:30301?discport=0",
  enr: "enr:-J-4QCbTarP2EJT714qRc2tGrJ-cXhqoDfd6sEOGv3HZC-AbBwPORLPeHV8zNR7pl9ZPRznZ9tx7fdvP14Rdti50K6-GAY-bcjEWg2V0aMrJhPxk7ASDEYwwgmlkgnY0gmlwhH8AAAGJc2VjcDI1NmsxoQNDOWAzKnzQKg4RWLvZ1ZBcV
gnE1aSu5EvcrIZkkgfUE4RzbmFwwIN0Y3CCd10",
  id: "1a13f0bbb189da1154f7e4846570d473cdebdedc815922ccae53c0bac5070926",
  ip: "127.0.0.1",
  listenAddr: "[::]:30301",
  name: "Geth/n1/v1.14.3-stable-ab48ba42/linux-amd64/go1.22.3",
  ports: {
    discovery: 0,
    listener: 30301
  },
  protocols: {
    eth: {
      config: {
        arrowGlacierBlock: 13773000,
        berlinBlock: 12244000,
        byzantiumBlock: 4370000,
        cancunTime: 1710338135,
        chainId: 1,
        constantinopleBlock: 7280000,
        daoForkBlock: 1920000,
        daoForkSupport: true,
        eip150Block: 2463000,
        eip155Block: 2675000,
        eip158Block: 2675000,
        ethash: {},
        grayGlacierBlock: 15050000,
        homesteadBlock: 1150000,
        istanbulBlock: 9069000,
        londonBlock: 12965000,
        muirGlacierBlock: 9200000,
        petersburgBlock: 7280000,
        shanghaiTime: 1681338455,
        terminalTotalDifficulty: 5.875e+22,
        terminalTotalDifficultyPassed: true
      },
      difficulty: 17179869184,
      genesis: "0xd4e56740f876aef8c010b86a40d5f56745a118d0906a34e69aec8c0db1cb8fa3",
      head: "0xd4e56740f876aef8c010b86a40d5f56745a118d0906a34e69aec8c0db1cb8fa3",
      network: 1900
    },
    snap: {}
  }
}
>
```

In teminal 5 and 6:

```
admin.addPeer("enode:...")
```

```
> exit
morteza@Rashidkhan:~/Desktop/My_PC/Crypto/CA2$ geth attach http://127.0.0.1:8002
WARN [05-21|18:18:33.491] Enabling deprecated personal namespace
Welcome to the Geth JavaScript console!

instance: Geth/n2/v1.14.3-stable-ab48ba42/linux-amd64/go1.22.3
at block: 0 (Thu Jan 01 1970 03:30:00 GMT+0330 (+0330))
 datadir: /home/morteza/Desktop/My_PC/Crypto/CA2/node02
 modules: admin:1.0 debug:1.0 eth:1.0 miner:1.0 net:1.0 personal:1.0 rpc:1.0 web3:1.0

To exit, press ctrl-d or type exit
> admin.addPeer("enode://433960332a7cd02a0e1158bbd995905c5609c495a4aee44bdcac86649207d4137fc23245d9676202900abc0ff5e007c2c202a35e71e36472ecf82b18367c5f87@127.0.0.1:30301?discport=0")
true
```

```
> exit
morteza@Rashidkhan:~/Desktop/My_PC/Crypto/CA2$ geth attach http://127.0.0.1:8003
WARN [05-21|18:19:09.275] Enabling deprecated personal namespace
Welcome to the Geth JavaScript console!

instance: Geth/n3/v1.14.3-stable-ab48ba42/linux-amd64/go1.22.3
at block: 0 (Thu Jan 01 1970 03:30:00 GMT+0330 (+0330))
 datadir: /home/morteza/Desktop/My_PC/Crypto/CA2/node03
 modules: admin:1.0 debug:1.0 eth:1.0 miner:1.0 net:1.0 personal:1.0 rpc:1.0 web3:1.0

To exit, press ctrl-d or type exit
> admin.addPeer("enode://433960332a7cd02a0e1158bbd995905c5609c495a4aee44bdcac86649207d4137fc23245d9676202900abc0ff5e007c2c202a35e71e36472ecf82b18367c5f87@127.0.0.1:30301?discport=0")
true
```

In terminal 4:

```
net.peerCount
```

```
morteza@Rashidkhan:~/Desktop/My_PC/Crypto/CA2$ geth attach http://127.0.0.1:8001
WARN [05-21|18:19:55.789] Enabling deprecated personal namespace
Welcome to the Geth JavaScript console!

instance: Geth/n1/v1.14.3-stable-ab48ba42/linux-amd64/go1.22.3
at block: 0 (Thu Jan 01 1970 03:30:00 GMT+0330 (+0330))
 datadir: /home/morteza/Desktop/My_PC/Crypto/CA2/node01
 modules: admin:1.0 debug:1.0 eth:1.0 miner:1.0 net:1.0 personal:1.0 rpc:1.0 web3:1.0

To exit, press ctrl-d or type exit
> net.peerCount
2
```

```
eth.getBalance(eth.accounts[0])

personal.unlockAccount(eth.accounts[0])
```

```
> net.peerCount
2
> eth.getBalance(eth.accounts[0])
10000000000810899055
> personal.unlockAccount(eth.accounts[0])
Unlock account 0x3c9fe79771d6f656167479b8beaf926169d841bd
Passphrase:
true
>
```

```
> eth.sendTransaction({from:eth.accounts[0], to:"0x409cd0e3fcbfb2d6fd1c9d02ec1ac0a46170b360", value:1000})
"0x2da9996e3d463036d9d9ae6579813fbdcb04d4976fbd4ac468c3adc7e0561809"
>
```

Make a new account for mining prize:

```
> personal.newAccount()
Passphrase:
Repeat passphrase:
"0x2140ea89b1dd9434b2038a6708005fc4a8a521a6"
> eth.accounts
["0x3833f34f72c9d44cd135c3e0ea907afd484c50eb", "0x2140ea89b1dd9434b2038a6708005fc4a8a521a6"]
> eth.getBalance(eth.accounts[1])
0
> miner.setEtherbase(eth.accounts[1])
true
> miner.start
function()
> miner.start(1)
null
> miner.start()
null
> miner.stop
function()
> miner.stop()
true
> miner.start()
null
> miner.start(2)
null
```

```
INFO [05-22|18:12:21] Successfully sealed new block           number=8 hash=c34381…ccd1ed
INFO [05-22|18:12:21] 🔗 block reached canonical chain         number=3 hash=539dc2…2d08ba
INFO [05-22|18:12:21] 🔨 mined potential block                 number=8 hash=c34381…ccd1ed
INFO [05-22|18:12:21] Commit new mining work                  number=9 txs=0 uncles=0 elapsed=157.651µs
INFO [05-22|18:12:21] Successfully sealed new block           number=9 hash=22b9d5…f3ad05
INFO [05-22|18:12:21] 🔗 block reached canonical chain         number=4 hash=fdc888…475d90
INFO [05-22|18:12:21] 🔨 mined potential block                 number=9 hash=22b9d5…f3ad05
INFO [05-22|18:12:21] Commit new mining work                  number=10 txs=0 uncles=0 elapsed=130.368µs
INFO [05-22|18:12:24] Successfully sealed new block           number=10 hash=7e7dd2…4c1387
INFO [05-22|18:12:24] 🔗 block reached canonical chain         number=5  hash=3e0c77…5943b4
INFO [05-22|18:12:24] 🔨 mined potential block                 number=10 hash=7e7dd2…4c1387
INFO [05-22|18:12:24] Commit new mining work                  number=11 txs=0 uncles=0 elapsed=205.346µs
INFO [05-22|18:12:25] Successfully sealed new block           number=11 hash=9cd20b…6f5f9b
INFO [05-22|18:12:25] 🔗 block reached canonical chain         number=6  hash=b30f2e…44348c
INFO [05-22|18:12:25] 🔨 mined potential block                 number=11 hash=9cd20b…6f5f9b
INFO [05-22|18:12:25] Commit new mining work                  number=12 txs=0 uncles=0 elapsed=199.052µs
INFO [05-22|18:12:27] Successfully sealed new block           number=12 hash=a925fa…36a558
INFO [05-22|18:12:27] 🔗 block reached canonical chain         number=7  hash=706358…d0a545
INFO [05-22|18:12:27] 🔨 mined potential block                 number=12 hash=a925fa…36a558
INFO [05-22|18:12:27] Commit new mining work                  number=13 txs=0 uncles=0 elapsed=163.274µs
INFO [05-22|18:12:28] Successfully sealed new block           number=13 hash=44c04e…0700ae
INFO [05-22|18:12:28] 🔗 block reached canonical chain         number=8  hash=c34381…ccd1ed
INFO [05-22|18:12:28] 🔨 mined potential block                 number=13 hash=44c04e…0700ae
INFO [05-22|18:12:28] Commit new mining work                  number=14 txs=0 uncles=0 elapsed=129.975µs
INFO [05-22|18:12:31] Successfully sealed new block           number=14 hash=558ed7…2365f0
INFO [05-22|18:12:31] 🔗 block reached canonical chain         number=9  hash=22b9d5…f3ad05
INFO [05-22|18:12:31] 🔨 mined potential block                 number=14 hash=558ed7…2365f0
INFO [05-22|18:12:31] Commit new mining work                  number=15 txs=0 uncles=0 elapsed=184.727µs
INFO [05-22|18:12:33] Successfully sealed new block           number=15 hash=74bbd5…75fc90
INFO [05-22|18:12:33] 🔗 block reached canonical chain         number=10 hash=7e7dd2…4c1387
INFO [05-22|18:12:33] 🔨 mined potential block                 number=15 hash=74bbd5…75fc90
INFO [05-22|18:12:33] Commit new mining work                  number=16 txs=0 uncles=0 elapsed=186.514µs
INFO [05-22|18:12:38] Successfully sealed new block           number=16 hash=e9ddd7…cf3158
INFO [05-22|18:12:38] 🔗 block reached canonical chain         number=11 hash=9cd20b…6f5f9b
INFO [05-22|18:12:38] 🔨 mined potential block                 number=16 hash=e9ddd7…cf3158
INFO [05-22|18:12:38] Commit new mining work                  number=17 txs=0 uncles=0 elapsed=206.39µs
INFO [05-22|18:12:43] Successfully sealed new block           number=17 hash=607dc2…753329
INFO [05-22|18:12:43] 🔗 block reached canonical chain         number=12 hash=a925fa…36a558
INFO [05-22|18:12:43] 🔨 mined potential block                 number=17 hash=607dc2…753329
INFO [05-22|18:12:43] Commit new mining work                  number=18 txs=0 uncles=0 elapsed=146.895µs
INFO [05-22|18:12:45] Successfully sealed new block           number=18 hash=67bbeb…255593
INFO [05-22|18:12:45] 🔗 block reached canonical chain         number=13 hash=44c04e…0700ae
INFO [05-22|18:12:45] 🔨 mined potential block                 number=18 hash=67bbeb…255593
INFO [05-22|18:12:45] Commit new mining work                  number=19 txs=0 uncles=0 elapsed=171.735µs
INFO [05-22|18:12:50] Successfully sealed new block           number=19 hash=a0d7c4…85dba4
INFO [05-22|18:12:50] 🔗 block reached canonical chain         number=14 hash=558ed7…2365f0
INFO [05-22|18:12:50] 🔨 mined potential block                 number=19 hash=a0d7c4…85dba4
INFO [05-22|18:12:50] Commit new mining work                  number=20 txs=0 uncles=0 elapsed=148.259µs
```

After mining account[1] balances has changed:

```
> eth.getBalance(eth.accounts[1])
0
> miner.setEtherbase(eth.accounts[1])
true
> miner.start
function()
> miner.start(1)
null
> miner.start()
null
> miner.stop
function()
> miner.stop()
true
> miner.start()
null
> miner.start(2)
null
> eth.getBalance(eth.accounts[1])
215000378000000000000
>
```

In termial 5:

```
> eth.sendTransaction({from:eth.accounts[0], to:"fa1eda41af21ee951fe4253bfffab304221dcdf3", value:1000})
"0xef0693ad609a41b6f7760a1a61cb9a007198097b3696f6c62fb5d817efe0d91d"
> eth.getBalance(eth.accounts[0])
1999622000810898055
> eth.pendingTransactions
[]
>
```

In termial 6: After above transaction

```
}
> eth.getBalance(eth.accounts[0])
1500000000810900055
>
```

.1

نود بلاکچینی (BlockChain Node) در واقع کامپیوتر یا دستگاهی است که به شبکه بلاکچین متصل می‌شود و در حفظ یکپارچگی سیستم مشارکت می‌کند. هر نود یک کپی از دفتر کل بلاکچین را نگه می‌دارد، تراکنش‌های جدید را صحت‌سنجی می‌کند، و در مکانیزم اجماع که امنیت شبکه را تأمین می‌کند مشارکت دارد. به عبارت دیگر، نود یکی از اجزای بنیادین سازنده شبکه بلاکچین است و بدون آن، بلاکچین نمی‌تواند درست کار کند.

نودهای بلاکچین برای این‌که مطمئن شوند نسخه یکسانی از دفتر کل بلاکچین را نگه داشته‌اند با هم در ارتباط هستند. این ارتباط از طریق فرآیندی تحت عنوان شبکه‌سازی همتا به همتا (peer-to-peer) انجام می‌شود که در آن، هر نود

فهرستی از سایر نودهایی که به آن‌ها متصل است نگه می‌دارد و اطلاعات را با آن‌ها مبادله می‌کند. وقتی تراکنش جدیدی شروع می‌شود، به کل شبکه مخابره می‌شود و هر نودی که آن را دریافت می‌کند، پیش از اضافه کردن آن به نسخه بلاکچین خود، آن را صحت‌سنجی می‌کند.

همچنین وقتی بلاک جدیدی استخراج و به زنجیره اضافه می‌شود، تمام نودها نسخه دفتر کل خود را به‌روز می‌کنند تا وضعیت جدید شبکه را به نمایش بگذارند. نودها به این شیوه در کنار هم کار می‌کنند تا امنیت، یکپارچگی و درستی سیستم بلاکچین را تضمین کنند.

فول نود (Full Node) یا گره کامل

فول نود یا نود کامل در شبکه بلاکچین به نودهایی گفته می‌شود که یک نسخه کامل از دفتر کل بلاکچین را نگهداری می‌کنند و مسئولیت اعتبارسنجی و تأیید تراکنش‌ها را روی شبکه بر عهده دارند. این نودها می‌توانند تراکنش‌ها و بلاک‌های جدید را به سایر نودهای روی شبکه مخابره (broadcast) کنند. فول نودها به منابع سخت‌افزاری قوی و فضای ذخیره‌سازی زیادی نیاز دارند و برای حفظ یکپارچگی و امنیت شبکه ضروری هستند.

لایت نود (Light Node) یا نودSPV

لایت نود یا نود سبک (که به آن نود SPV یا Simplified Payment Verification هم می‌گویند) یک نسخه سبک از فول نود است که نسخه کامل بلاکچین را نگهداری نمی‌کند. در عوض، نودهای سبک برای تأیید تراکنش‌ها به سایر نودها وابسته‌اند و فقط بخشی از اطلاعات بلاکچین را نگه می‌دارند. این ویژگی باعث شده تا منابع کمتری مصرف کنند اما به همین علت در مقایسه با فول نودها امنیت کمتری دارند.

.2

وقتی این دستور را اجرا می کنیم عبارت null چاپ می شود که به معنای آن است که این نود بدون خطا شروع به mining کرده است. اگر به terminal 4 برویم یعنی جایی که نود را استارت کردیم یه سری لاگ داریم که نشان دهنده روند ماین کردن و تعداد ترنسکشن های داخل بلاک ماین شده است.

```
INFO [05-22|18:12:31] Successfully sealed new block        number=14 hash=558ed7…2365f0
INFO [05-22|18:12:31] 🔗 block reached canonical chain      number=9  hash=22b9d5…f3ad05
INFO [05-22|18:12:31] 🔨 mined potential block              number=14 hash=558ed7…2365f0
INFO [05-22|18:12:31] Commit new mining work               number=15 txs=0 uncles=0 elapsed=184.727µs
INFO [05-22|18:12:33] Successfully sealed new block        number=15 hash=74bbd5…75fc90
INFO [05-22|18:12:33] 🔗 block reached canonical chain      number=10 hash=7e7dd2…4c1387
INFO [05-22|18:12:33] 🔨 mined potential block              number=15 hash=74bbd5…75fc90
```

.3

خیر- برا ی ایجاد یک بلوک معتبر در شبکه اتریوم، باید اعتبار خود را اثبات کنیم، که به طور کلی به عنوان Work of Proof شناخته می شود. این به معنای این است که باید یک مقدار nonce را پیدا کنیم که هش بلوک با توجه به آن، یک الگوریتم خاص مانند Ethash در اتریوم را اعمال میکند و نتیجه آن یک عدد خاص می باشد. این فرایند به طور تصادفی انجام می شود و این امکان وجود ندارد که بتوانیم به سرعت بلوک های معتبر را ایجاد کنیم. حتی اگر بتوانیم بلوک های معتبر را در بلاکچین لوکال خود ایجاد کنیم، برای اعلام این بلوک ها به عنوان بخشی از زنجیره اصلی اتریوم، باید بتوانیم این بلوکها را در شبکه اتریوم به اشتراک بگذاریم. این امر نیازمند ارتباط با سایر نودهای شبکه اتریوم، ارسا ل بلوک ها به شبکه و دریافت تأییدات از دیگر ماینرها و نودها است. این ارتباطات به دلیل تنظیمات امنیتی شبکه اتریوم و استانداردهای پروتکل اتریوم امکانپذیر نیست.

پس باتوجه به توضیحات بالا عملا این امکان وجود ندارد.