Ethereum

for noobs

Ethereum network protocol

Hội anh em blockchain "thiện lành"
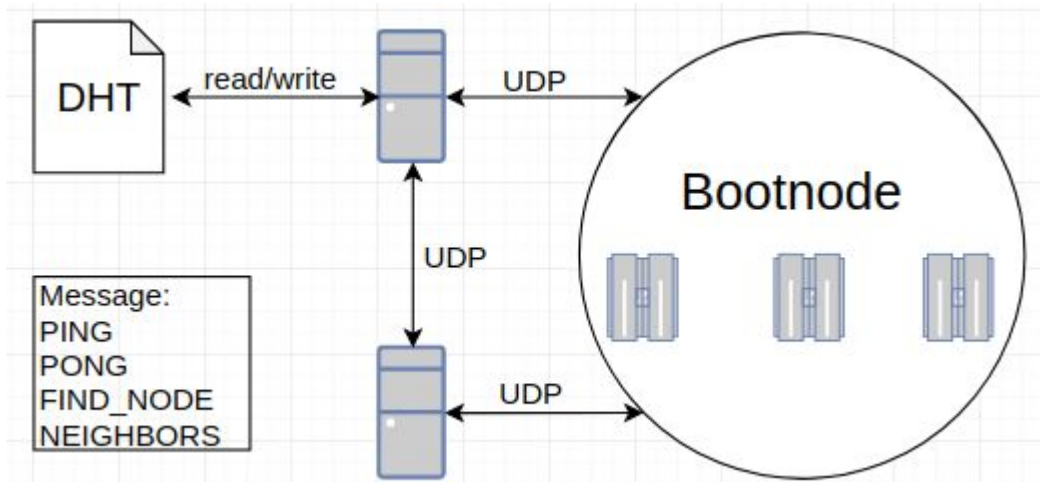
Contents

- Peer discover

- Ethereum Protocol

- Demo code

INFINITY
BLOCKCHAIN LABS

Peer discovery

Kademlia-like

- A node is identified by an ID that is its public key.
- Distance between two nodes is the bitwise exclusive XOR of the hashes of the IDs.


```
21   var MainnetBootnodes = []string{
22       // Ethereum Foundation Go Bootnodes
23       "enode://a979fb575495b8d6db44f750317d0f4622bf4c2aa3365d6af7c284339968eef29b69ad0dce72a4d8db5ebb4968de0e3bec910127f134779fbcb0cb6d3331163c@52.16.188.185:3030
24       "enode://3f1d12044546b76342d59d4a05532c14b85aa669704bfe1f864fe079415aa2c02d743e03218e57a33fb94523adb54032871a6c51b2cc5514cb7c7e35b3ed0a99@13.93.211.84:30303
25       "enode://78de8a0916848093c73790ead81d1928bec737d565119932b98c6b100d944b7a95e94f847f689fc723399d2e31129d182f7ef3863f2b4c820abbf3ab2722344d@191.235.84.50:3030
26       "enode://158f8aab45f6d19c6cbf4a089c2670541a8da11978a2f90dbf6a502a4a3bab80d288afdbeb7ec0ef6d92de563767f3b1ea9e8e334ca711e9f8e2df5a0385e8e6@13.75.154.138:3030
27       "enode://1118980bf48b0a3640bdba04e0fe78b1add18e1cd99bf22d53daac1fd9972ad650df52176e7c7d89d1114cfef2bc23a2959aa54998a46afcf7d91809f0855082@52.74.57.123:30303
28
29       // Ethereum Foundation C++ Bootnodes
30       "enode://979b7fa28feeb35a4741660a16076f1943202cb72b6af70d327f053e248bab9ba81760f39d0701ef1d8f89cc1fbd2cacba0710a12cd5314d5e0c9021aa3637f9@5.1.83.226:30303",
31   }
```

https://github.com/ethereum/devp2p/blob/master/discv5/discv5.md

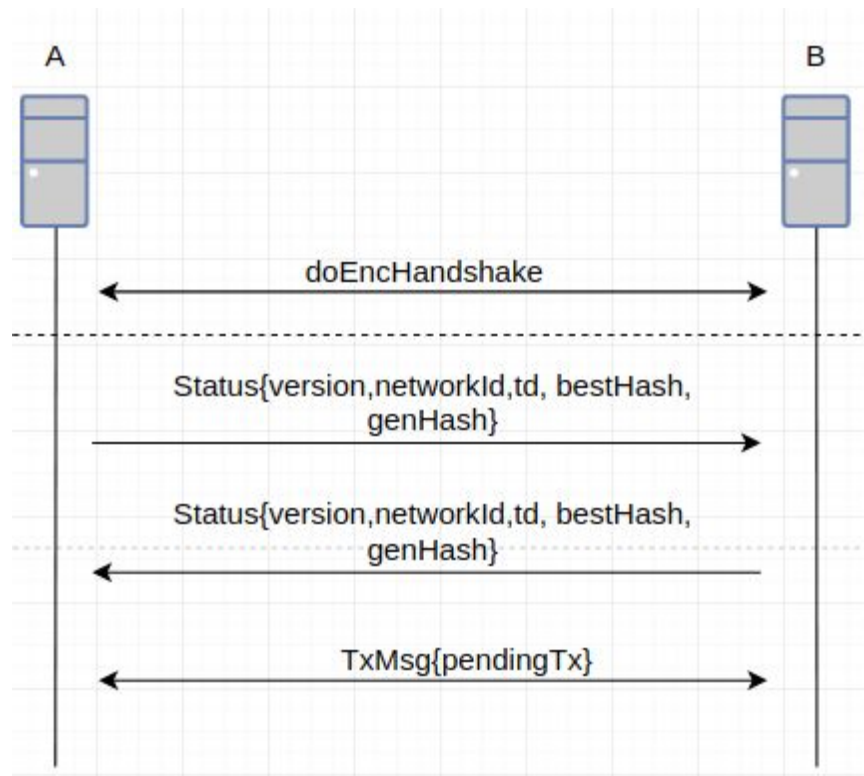go-ethereum/params/bootnodes.go

Peer protocol
Messages

- **Status(0x00)**
  [protocolVersion, networkId, td, bestHash, genesisHash]

- **NewBlockHashes (0x01)**
  [[hash_0, number_0], ...]

- **Transactions (0x02)**
  [[tx], ...]

- **GetBlockHeaders (0x03)**
  [block, maxHeaders, skip, reverse]

- **BlockHeaders (0x04)**
  [blockHeader_0, ...]

- **GetBlockBodies (0x05)**
  [hash_0, ...]

- **BlockBodies (0x06)**
  [[transactions_0, uncles_0] , ...]

https://github.com/ethereum/devp2p/blob/master/caps/eth.md

- **NewBlock (0x07)**
  [[blockHeader, transactionList, uncleList], totalDifficulty]

- **GetNodeData (0x0d)**
  [hash_0, hash_1,, ...]

- **NodeData (0x0e)**
  [value_0, value_1.]

- **GetReceipts (0x0f)**
  [blockHash_0, ...]

- **Receipts (0x10)**
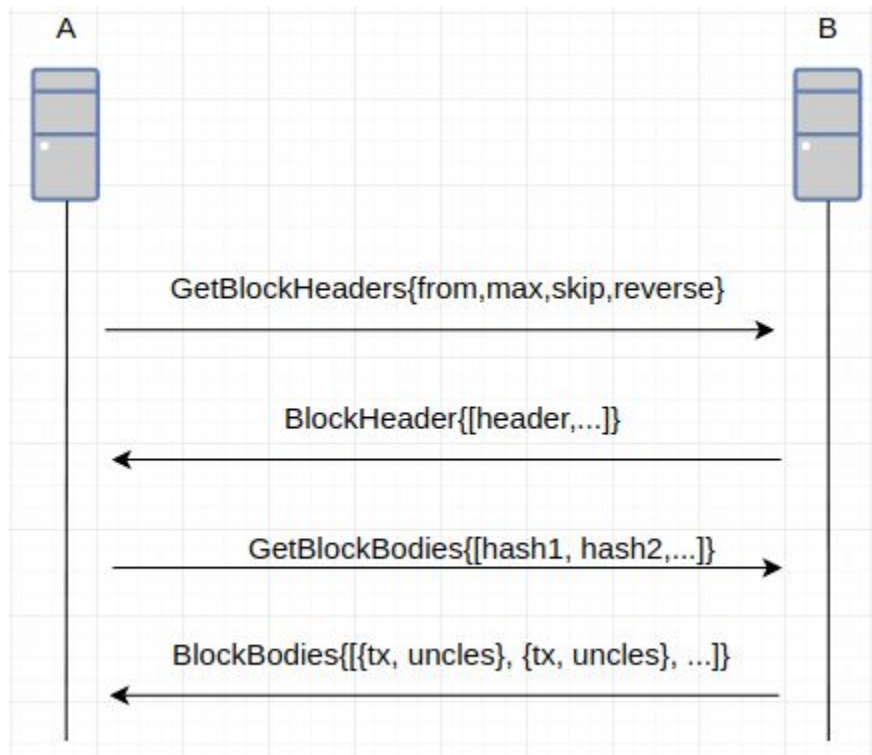 [[receipt_0,...], ...]

Peer protocol

Handshake

- Exchange key.
- Exchange blockchain status information.
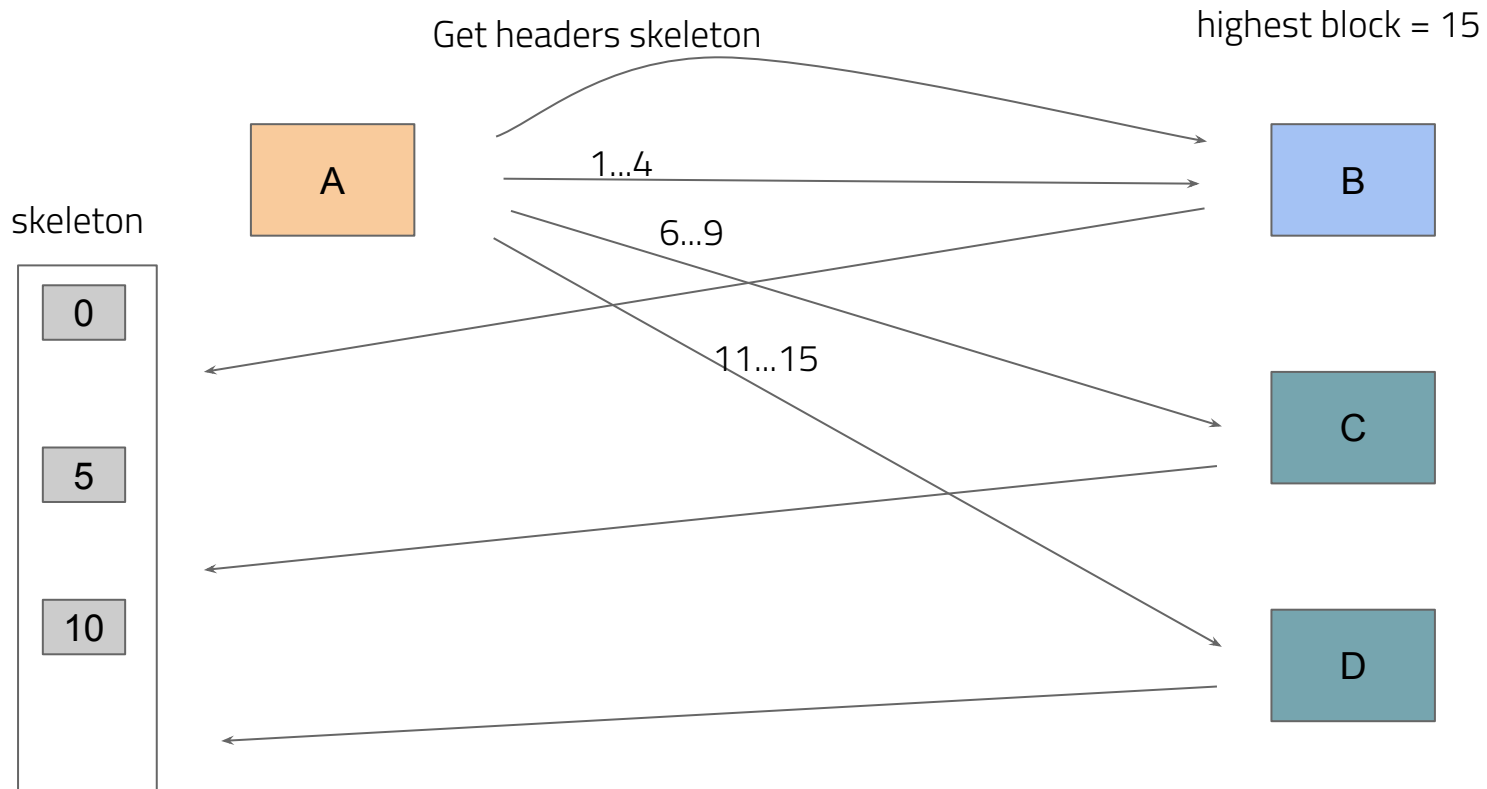- Pending transactions broadcast.

Peer protocol

Sync data

- Compare total difficulty
- Calculate pivot
- Download block headers skeleton
- Download block headers concurrently
- Download block bodies concurrently

Peer protocol

Get headers skeleton

highest block = 15

A

skeleton

B

0

1...4

6...9

5

11...15

C

10

D

INFINITY
BLOCKCHAIN LABS

Code demo

Connect to a fullnode by peer protocol

https://github.com/phukq/ethnoob-geth-example/tree/master/protocol

INFINITY
BLOCKCHAIN LABS