NPTEL ONLINE CERTIFICATION COURSES

Blockchain and its applications

Bishakh Chandra Ghosh

Department of Computer Science & Engineering
Indian Institute of Technology Kharagpur

Lecture 23: Ethereum 2

CONCEPTS COVERED

- Obtaining Ethereum for testnets
- Unlocking account
- Geth transactions using RPC over HTTP

KEYWORDS

- Ethereum Transactions
- Gas
- Faucet

Query Balance

Ensure Geth is running.

Querying the balance of an account:
POST request to the HTTP endpoint (default: 127.0.0.1:8545)

JSON Payload:

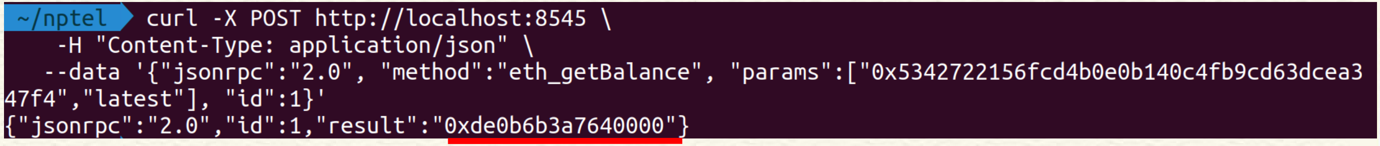
```
{
"jsonrpc": "2.0",
"method": "eth_getBalance",
"params": [
"0x9808f22453Ee87cc23eA76ca7Ed66a4F294d54D4",
"latest"
],
"id": 1
}
```

Query Balance

Querying the balance of an account:

POST request using curl:

```
curl -X POST http://localhost:8545 \
-H "Content-Type: application/json" \
--data '{"jsonrpc":"2.0", "method":"eth_getBalance", "params":
["0x5342722156fcd4b0e0b140c4fb9cd63dcea347f4","latest"],
"id":1}'
```



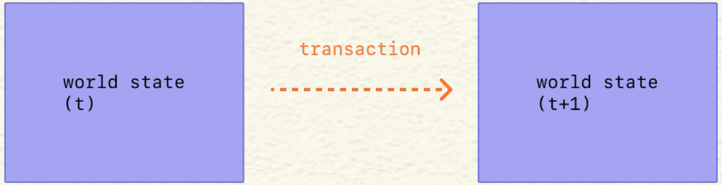
```
~/nptel  curl -X POST http://localhost:8545 \
    -H "Content-Type: application/json" \
   --data '{"jsonrpc":"2.0", "method":"eth_getBalance", "params":["0x5342722156fcd4b0e0b140c4fb9cd63dcea3
47f4","latest"], "id":1}'
{"jsonrpc":"2.0","id":1,"result":"0xde0b6b3a7640000"}
```

Ethereum Transactions

- Transactions are **cryptographically signed instructions from accounts**.

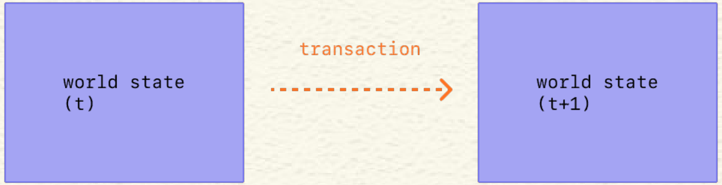
- An account will initiate a transaction to update the state of the Ethereum network.

- The simplest transaction is transferring ETH from one account to another.



Ethereum Transactions

- Transactions are **cryptographically signed instructions from accounts.**
- An account will initiate a transaction to update the state of the Ethereum network.
- The simplest transaction is transferring ETH from one account to another.



Requires:
1. Access to account private key
2. Gas

Gas

- Each Ethereum **transaction requires computational resources** to execute.

- Each transaction requires a **fee**.

- **Gas refers to the fee required to conduct a transaction on Ethereum successfully.**

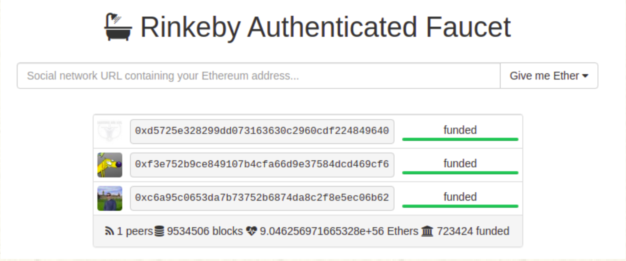
- Gas is paid as amounts of Ethers.

Get ether in testnet

- For executing transactions in a testnet, we can obtain ethers from faucet.

- Goerli faucet:
  - Social faucet: https://faucet.goerli.mudit.blog/
  - Simple faucet: https://goerli-faucet.slock.it/

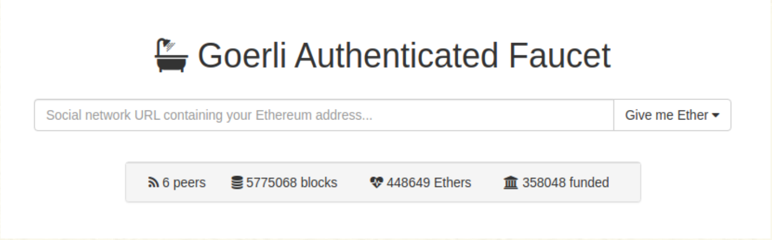
- Rinkeby faucet: https://faucet.rinkeby.io/



Rinkeby Authenticated Faucet

0xd5725e328299dd073163630c2960cdf224849640	funded
0xf3e752b9ce849107b4cfa66d9e37584dcd469cf6	funded
0xc6a95c0653da7b73752b6874da8c2f8e5ec06b62	funded

1 peers 9534506 blocks 9.046256971665328e+56 Ethers 723424 funded

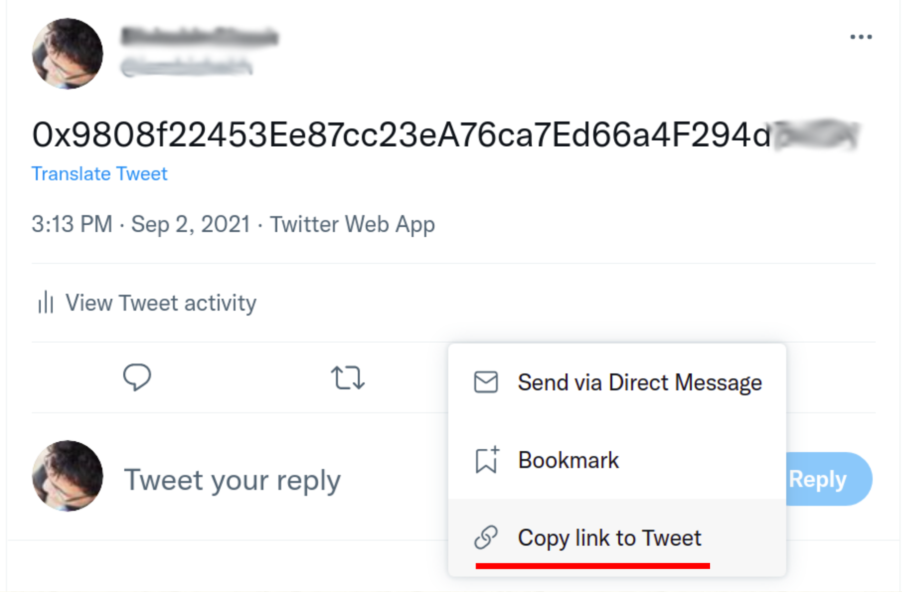


Goerli Authenticated Faucet

6 peers 5775068 blocks 448649 Ethers 358048 funded

Get ether in Goerli testnet

- Post a tweet containg ethereum account address.



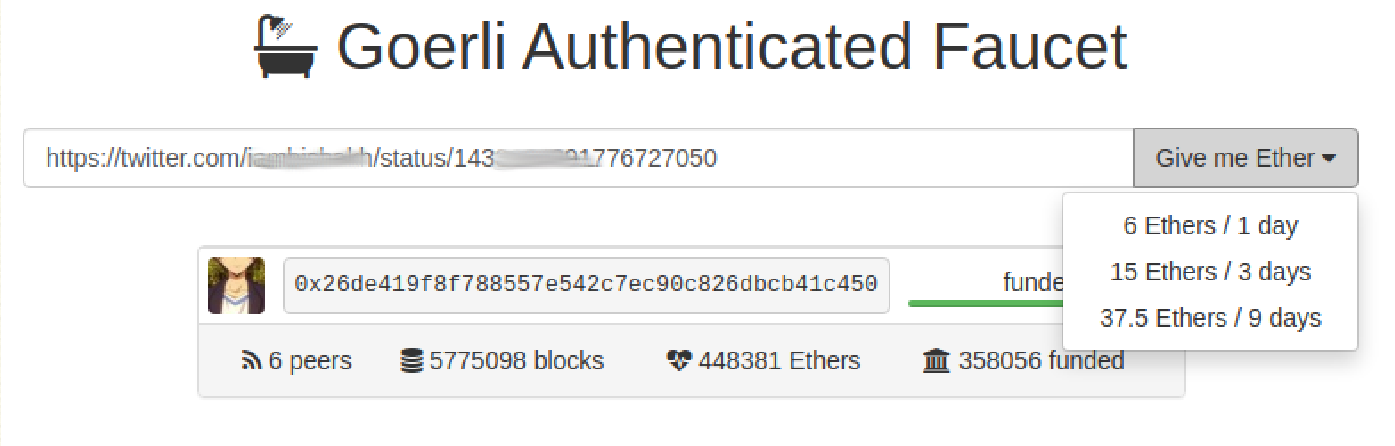
[redacted]

0x9808f22453Ee87cc23eA76ca7Ed66a4F294d[redacted]

3:13 PM · Sep 2, 2021 · Twitter Web App

Get ether in Goerli testnet

- Paste tweet link in faucet.



Goerli Authenticated Faucet

https://twitter.com/i[redacted]h/status/143[redacted]776727050

0x26de419f8f788557e542c7ec90c826dbcb41c450 funde

6 peers 5775098 blocks 448381 Ethers 358056 funded

Unlock Account

- Create new account for goerli testnet, suppose password is set to "123"
- Write account password in a text file. Here we name it pwd.txt

```
geth --goerli account new
echo "123" > pwd.txt
```

- Unlock account while starting geth

```
geth --goerli --syncmode "light" --http --allow-insecure-unlock --unlock
d84a0607843b28c3f468857f82f784d9ff743bf8 --password pwd.txt
```

eth_sendTransaction

POST sendTransaction
Creates new message call transaction or a contract creation, if the data field contains code.

Parameters
Object - The transaction object
from: DATA, 20 Bytes - The address the transaction is send from.
to: DATA, 20 Bytes -The address the transaction is directed to.
gas: QUANTITY - (optional, default: 90000) Integer of the gas provided for the transaction execution. It will return unused gas.
gasPrice: QUANTITY - (optional, default: To-Be-Determined) The gasPrice used for each paid gas
value: QUANTITY - (optional) Integer of the value sent with this transaction
data: DATA - The compiled code of a contract OR the hash of the invoked method signature and encoded parameters. For details see Ethereum Contract ABI
nonce: QUANTITY - (optional) Integer of a nonce. This allows to overwrite your own pending transactions that use the same nonce.

Returns
DATA, 32 Bytes - the transaction hash, or the zero hash if the transaction is not yet available.

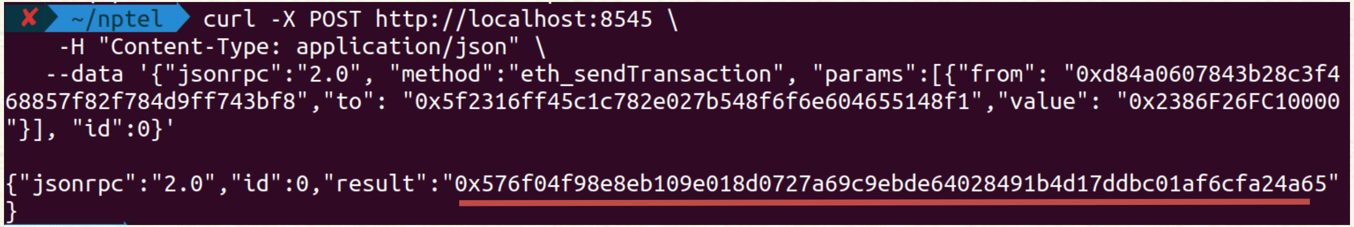
Prepare Transaction

```
{
"jsonrpc": "2.0",
"method": "eth_sendTransaction",
"params": [
{
"from":
"0xd84a0607843b28c3f468857f82f784d9ff743bf8"
,
"to":
"0x5f2316ff45c1c782e027b548f6f6e604655148f1"
,
"value": "0x2386F26FC10000"
}
],
"id": 0
}
```

0.1 eth

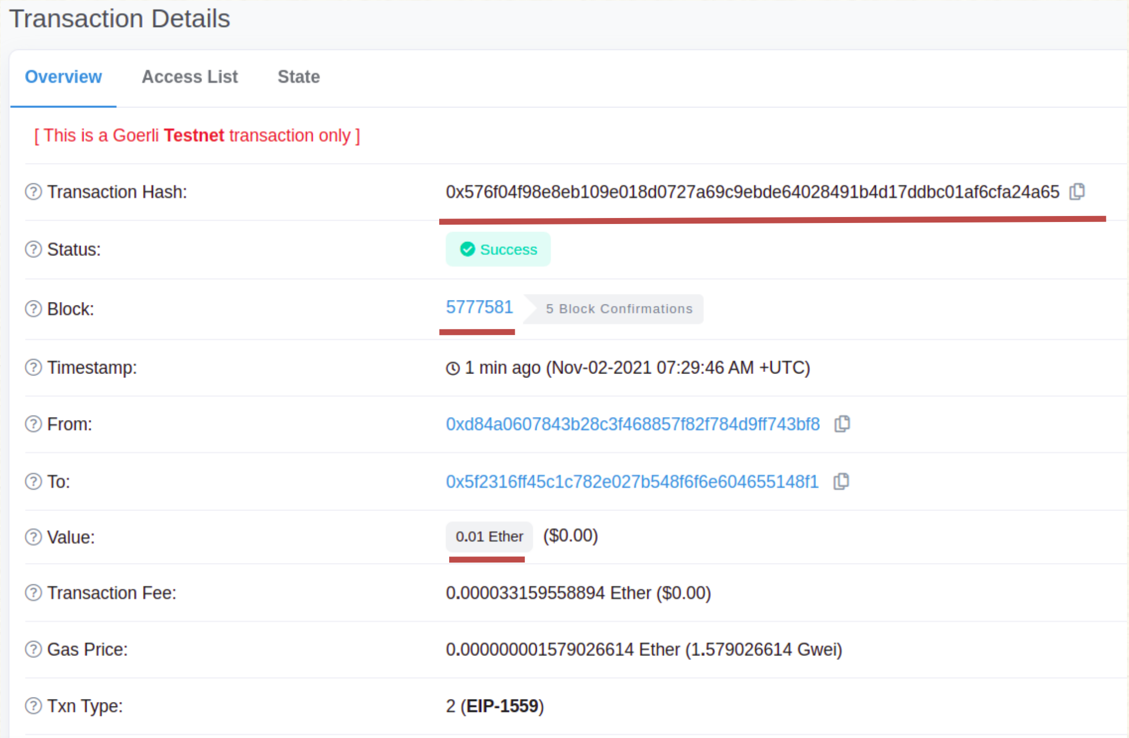
Submit Transaction

```
curl -X POST http://localhost:8545 \
-H "Content-Type: application/json" \
--data '{"jsonrpc":"2.0", "method":"eth_sendTransaction", "params":[{"from":
"0xd84a0607843b28c3f468857f82f784d9ff743bf8","to":
"0x5f2316ff45c1c782e027b548f6f6e604655148f1","value":
"0x2386F26FC10000"}], "id":0}'
```



```
✗ ~/nptel curl -X POST http://localhost:8545 \
    -H "Content-Type: application/json" \
   --data '{"jsonrpc":"2.0", "method":"eth_sendTransaction", "params":[{"from": "0xd84a0607843b28c3f4
68857f82f784d9ff743bf8","to": "0x5f2316ff45c1c782e027b548f6f6e604655148f1","value": "0x2386F26FC10000
"}], "id":0}'

{"jsonrpc":"2.0","id":0,"result":"0x576f04f98e8eb109e018d0727a69c9ebde64028491b4d17ddbc01af6cfa24a65"
}
```

View Transaction on Etherscan



Transaction Details

Overview | Access List | State

[This is a Goerli **Testnet** transaction only]

? Transaction Hash:	0x576f04f98e8eb109e018d0727a69c9ebde64028491b4d17ddbc01af6cfa24a65
? Status:	✓ Success
? Block:	5777581 5 Block Confirmations
? Timestamp:	1 min ago (Nov-02-2021 07:29:46 AM +UTC)
? From:	0xd84a0607843b28c3f468857f82f784d9ff743bf8
? To:	0x5f2316ff45c1c782e027b548f6f6e604655148f1
? Value:	0.01 Ether ($0.00)
? Transaction Fee:	0.000033159558894 Ether ($0.00)
? Gas Price:	0.000000001579026614 Ether (1.579026614 Gwei)
? Txn Type:	2 (**EIP-1559**)

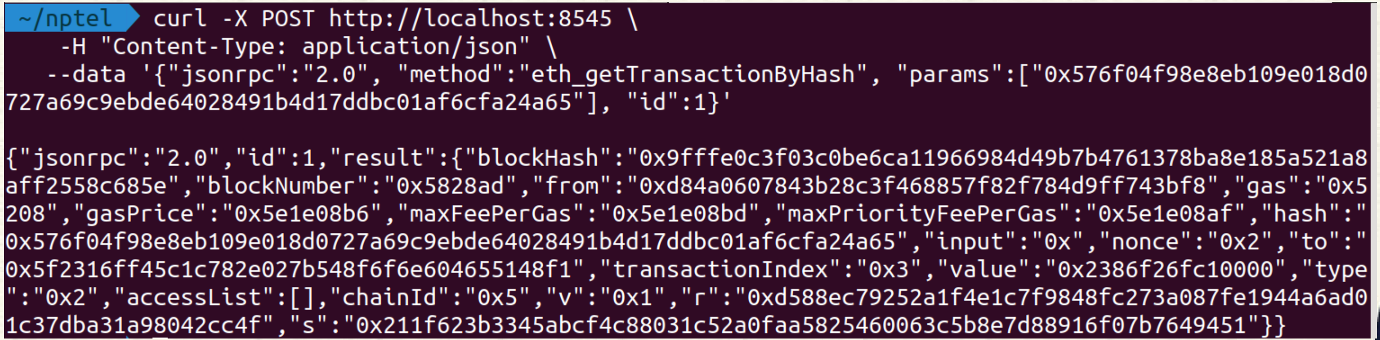
https://goerli.etherscan.io/

Get Transaction by Hash

```
{
"jsonrpc": "2.0",
"method": "eth_getTransactionByHash",
"params": [
"0x576f04f98e8eb109e018d0727a69c9ebde64028491b
4d17ddbc01af6cfa24a65"
],
"id": 1
}
```

Get Transaction by Hash

```
curl -X POST http://localhost:8545 \
-H "Content-Type: application/json" \
--data '{"jsonrpc":"2.0", "method":"eth_getTransactionByHash", "params":
["0x576f04f98e8eb109e018d0727a69c9ebde64028491b4d17ddbc01af6cfa24a65"],
"id":1}'
```



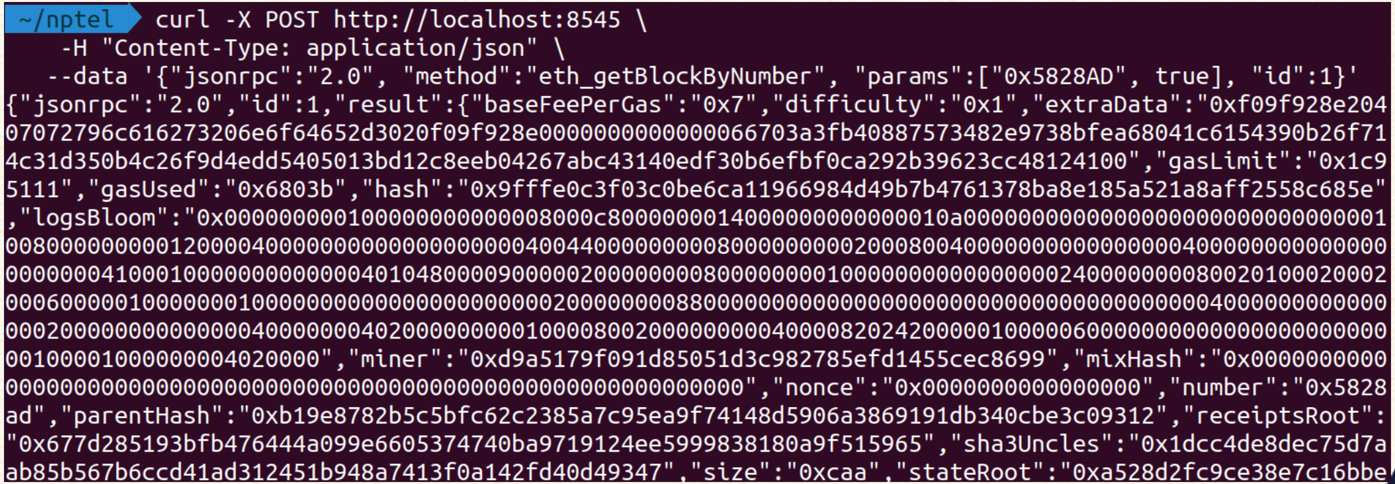
```
~/nptel  curl -X POST http://localhost:8545 \
    -H "Content-Type: application/json" \
   --data '{"jsonrpc":"2.0", "method":"eth_getTransactionByHash", "params":["0x576f04f98e8eb109e018d0
727a69c9ebde64028491b4d17ddbc01af6cfa24a65"], "id":1}'

{"jsonrpc":"2.0","id":1,"result":{"blockHash":"0x9fffe0c3f03c0be6ca11966984d49b7b4761378ba8e185a521a8
aff2558c685e","blockNumber":"0x5828ad","from":"0xd84a0607843b28c3f468857f82f784d9ff743bf8","gas":"0x5
208","gasPrice":"0x5e1e08b6","maxFeePerGas":"0x5e1e08bd","maxPriorityFeePerGas":"0x5e1e08af","hash":"
0x576f04f98e8eb109e018d0727a69c9ebde64028491b4d17ddbc01af6cfa24a65","input":"0x","nonce":"0x2","to":"
0x5f2316ff45c1c782e027b548f6f6e604655148f1","transactionIndex":"0x3","value":"0x2386f26fc10000","type
":"0x2","accessList":[],"chainId":"0x5","v":"0x1","r":"0xd588ec79252a1f4e1c7f9848fc273a087fe1944a6ad0
1c37dba31a98042cc4f","s":"0x211f623b3345abcf4c88031c52a0faa5825460063c5b8e7d88916f07b7649451"}}
```

Query Blocks

```
{
"jsonrpc": "2.0",
"method": "eth_getBlockByNumber",
"params": [
"0x5828AD",
true
],
"id": 1
}
```

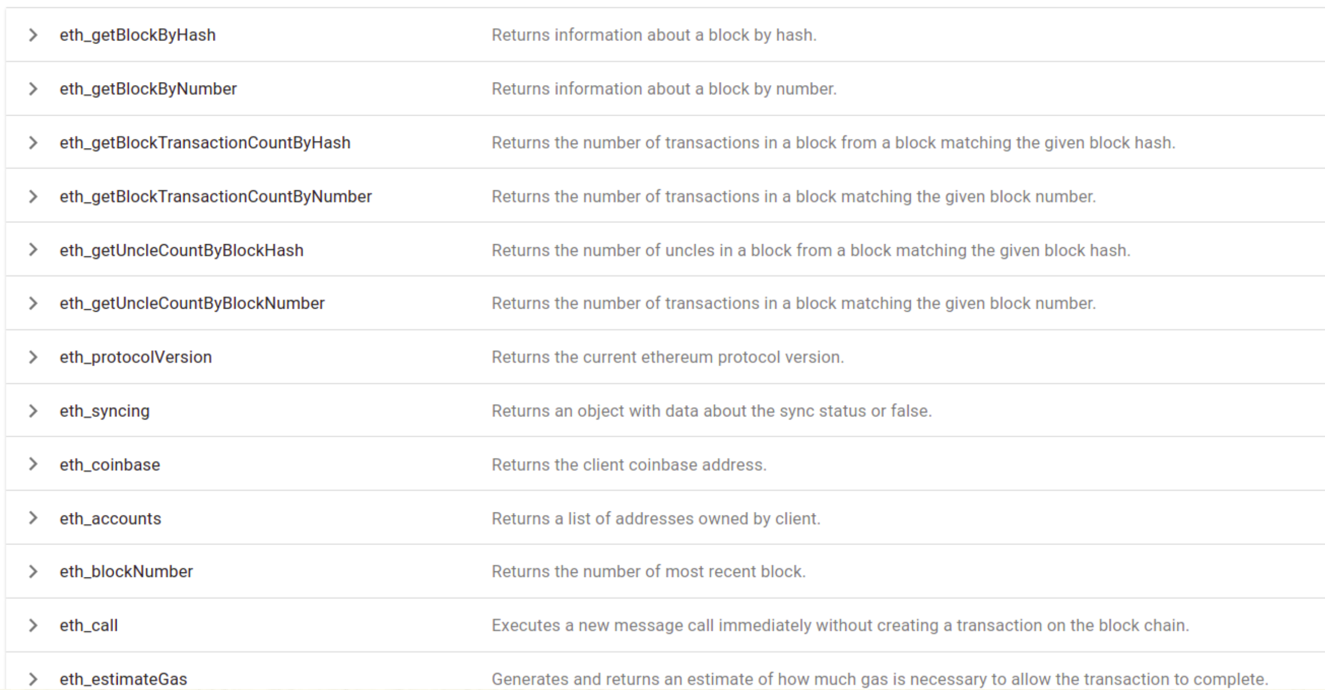
```
curl -X POST http://localhost:8545 \
-H "Content-Type: application/json" \
--data '{"jsonrpc":"2.0", "method":"eth_getBlockByNumber",
"params":["0x5828AD", true], "id":1}'
```

Query Blocks



```
~/nptel  curl -X POST http://localhost:8545 \
    -H "Content-Type: application/json" \
   --data '{"jsonrpc":"2.0", "method":"eth_getBlockByNumber", "params":["0x5828AD", true], "id":1}'
{"jsonrpc":"2.0","id":1,"result":{"baseFeePerGas":"0x7","difficulty":"0x1","extraData":"0xf09f928e204
07072796c616273206e6f64652d3020f09f928e0000000000000066703a3fb40887573482e9738bfea68041c6154390b26f71
4c31d350b4c26f9d4edd5405013bd12c8eeb04267abc43140edf30b6efbf0ca292b39623cc48124100","gasLimit":"0x1c9
5111","gasUsed":"0x6803b","hash":"0x9fffe0c3f03c0be6ca11966984d49b7b4761378ba8e185a521a8aff2558c685e"
,"logsBloom":"0x00000000010000000000008000c80000000140000000000000010a000000000000000000000000000000001
00800000000012000040000000000000000000000400440000080000000000002000800400000000000000040000000000000000
00000004100010000000000000401048000090000020000000008000000001000000000000000240000000080020100020002
00060000001000000001000000000000000000000200000000880000000000000000000000000000000000040000000000000
00020000000000000000400000004020000000000100008002000000040000820242000000100000600000000000000000000
00100001000000004020000","miner":"0xd9a5179f091d85051d3c982785efd1455cec8699","mixHash":"0x0000000000
000000000000000000000000000000000000000000000000000000","nonce":"0x0000000000000000","number":"0x5828
ad","parentHash":"0xb19e8782b5c5bfc62c2385a7c95ea9f74148d5906a3869191db340cbe3c09312","receiptsRoot":
"0x677d285193bfb476444a099e6605374740ba9719124ee5999838180a9f515965","sha3Uncles":"0x1dcc4de8dec75d7a
ab85b567b6ccd41ad312451b948a7413f0a142fd40d49347","size":"0xcaa","stateRoot":"0xa528d2fc9ce38e7c16bbe
```

Many More RPC Methods



eth_getBlockByHash	Returns information about a block by hash.
eth_getBlockByNumber	Returns information about a block by number.
eth_getBlockTransactionCountByHash	Returns the number of transactions in a block from a block matching the given block hash.
eth_getBlockTransactionCountByNumber	Returns the number of transactions in a block matching the given block number.
eth_getUncleCountByBlockHash	Returns the number of uncles in a block from a block matching the given block hash.
eth_getUncleCountByBlockNumber	Returns the number of transactions in a block matching the given block number.
eth_protocolVersion	Returns the current ethereum protocol version.
eth_syncing	Returns an object with data about the sync status or false.
eth_coinbase	Returns the client coinbase address.
eth_accounts	Returns a list of addresses owned by client.
eth_blockNumber	Returns the number of most recent block.
eth_call	Executes a new message call immediately without creating a transaction on the block chain.
eth_estimateGas	Generates and returns an estimate of how much gas is necessary to allow the transaction to complete.

https://playground.open-rpc.org/?schemaUrl=https://raw.githubusercontent.com/ethereum/eth1.0-apis/assembled-spec/openrpc.json

Conclusion

- Ethereum Transactions
- Obtaining Ether for testnets
- Unlocking Account
- Submit Transactions and monitor transactions

Thank you