Лабораторная работа №1

Работа с Bitcoin core.

Цель – изучить основные концепции Bitcoin core, научиться работать с bitcoin-cli.

Требования – развернутая среда для docker.

План работы:

Скачиваем докер-контейнер с нужной нам средой:

**sudo docker pull freewil/bitcoin-testnet-box**

Using default tag: latest

latest: Pulling from freewil/bitcoin-testnet-box

5d3b2c2d21bb: Pull complete

3fc2062ea667: Pull complete

75adf526d75b: Pull complete

af3aedc731a2: Pull complete

3d4518731c1c: Pull complete

efb53859728b: Pull complete

bda9c64dab28: Pull complete

074e898e3d08: Pull complete

49df3cdb2e58: Pull complete

569e1ff070a6: Pull complete

Digest: sha256:b347344f105c9345571c9abe00fff13f64a0332e7318dea332682f37d908a2ff

Status: Downloaded newer image for freewil/bitcoin-testnet-box:latest

docker.io/freewil/bitcoin-testnet-box:latest

Запускаем среду в докер-контейнере:

**user@machine:~$ sudo docker run -t -i -p 19001:19001 -p 19011:19011 freewil/bitcoin-testnet-box**

tester@3aa4b531c63a ~/bitcoin-testnet-box$

и по изменившемуся промпту понимаем, что мы теперь работаем в шелле контейнера

Запуск узлов:

**tester@d942757991b0 ~/bitcoin-testnet-box$ make start** – это скрипт, который просто запускает 2 экземпляра узла биткойна, настроенных на подкаталоги 1 и 2 (в которых находятся заранее заданные параметры конфигурации обоих узлов).

Запуск узла производится командой **bitcoind**, параметр **-datadir** задает рабочий каталог, в котором будут храниться данные узла, флаг **-daemon** означает, что ПО запускается как сервис (демон), т.е. запускается новый процесс, ожидающий обращения к нему.

**bitcoind -datadir=1 -daemon**

Bitcoin Core starting

**bitcoind -datadir=2 -daemon**

Bitcoin Core starting

Для работы с узлом биткойна используется утилита bitcoin-cli (Bitcoin command line interface).

Получение информации об узлах:

**tester@d942757991b0 ~/bitcoin-testnet-box$ bitcoin-cli -datadir=1 -getinfo**

выдает информацию о состоянии первого узла:

bitcoin-cli -datadir=1 -getinfo

{

"version": 210000,

"blocks": 0,

"headers": 0,

"verificationprogress": 1,

"timeoffset": 0,

"connections": {

"in": 1,

"out": 0,

"total": 1

},

"proxy": "",

"difficulty": 4.656542373906925e-10,

"chain": "regtest",

"relayfee": 0.00001000,

"warnings": ""

}

**tester@d942757991b0 ~/bitcoin-testnet-box$ bitcoin-cli -datadir=2 -getinfo**

соответственно, выдает информацию о состоянии второго узла

bitcoin-cli -datadir=2 -getinfo

{

"version": 210000,

"blocks": 0,

"headers": 0,

"verificationprogress": 1,

"timeoffset": 0,

"connections": {

"in": 0,

"out": 1,

"total": 1

},

"proxy": "",

"difficulty": 4.656542373906925e-10,

"chain": "regtest",

"relayfee": 0.00001000,

"warnings": ""

}

Исходя из информации о статусе узлов, мы видим, что сеть еще не работает – еще не создано ни одного блока. Но прежде, чем создавать блоки, создадим по одному кошельку в каждом узле.

**Создание кошельков**

Для того, чтобы работать со средствами в сети bitcoin, необходим кошелек. Кошелек создается также через утилиту **bitcoin-cli**. Создадим по кошельку для обоих узлов.

**tester@d942757991b0 ~/bitcoin-testnet-box$ bitcoin-cli -datadir=1 createwallet wallet1**

{

"name": "wallet1",

"warning": ""

}

**tester@d942757991b0 ~/bitcoin-testnet-box$ bitcoin-cli -datadir=2 createwallet wallet2**

{

"name": "wallet2",

"warning": ""

}

И после этого займемся генерацией блоков:

**Генерация блока**

Команда

**tester@d942757991b0 ~/bitcoin-testnet-box$ bitcoin-cli -datadir=1 -generate 1**

bitcoin-cli -datadir=1 -generate 1

{

"address": "bcrt1qs95764s45pq8cfjqkwj5c6awx0f6qepznkh6j8",

"blocks": [

"7d157c51f76f5a0faae4bb0613fd02ba182da35d0d05f4234984786f44718ab7"

]

}

сгенерирует 1 блок. На всякий случай, чтобы обеспечить средства для дальнейших переводов, намайним побольше:

**tester@d942757991b0 ~/bitcoin-testnet-box$ bitcoin-cli -datadir=1 -generate 200**

bitcoin-cli -datadir=1 -generate 200

{

"address": "bcrt1qgpzqxu9pdx3fwapws7llzetnum26szxjyex3nh",

"blocks": [

"0828a6d49f97033d4f80925996ccfcd63ccea57840e57b09c850d86cc6074304",

…

"082b3983e4fcf871b9e95ad110a372ae9e8a1a2a3beeda08b643932c5c2c162c"

]

}

После этого проверим состояние кошельков, сперва для первого узла, командой

**tester@d942757991b0 ~/bitcoin-testnet-box$ bitcoin-cli -datadir=1 -getinfo**

bitcoin-cli -datadir=1 -getinfo

{

"version": 210000,

"blocks": 201,

"headers": 201,

"verificationprogress": 1,

"timeoffset": 0,

"connections": {

"in": 1,

"out": 0,

"total": 1

},

"proxy": "",

"difficulty": 4.656542373906925e-10,

"chain": "regtest",

"keypoolsize": 999,

"paytxfee": 0.00000000,

**"balance": 5050.00000000,**

"relayfee": 0.00001000,

"warnings": ""

}

Обратите внимание, что счетчик блоков отображает количество намайненных блоков, а баланс- намайненные средства.

И затем проверим статус второго узла, командой

**tester@d942757991b0 ~/bitcoin-testnet-box$ bitcoin-cli -datadir=2 -getinfo**

bitcoin-cli -datadir=2 -getinfo

{

"version": 210000,

"blocks": 201,

"headers": 201,

"verificationprogress": 1,

"timeoffset": 0,

"connections": {

"in": 0,

"out": 1,

"total": 1

},

"proxy": "",

"difficulty": 4.656542373906925e-10,

"chain": "regtest",

"keypoolsize": 1000,

"paytxfee": 0.00000000,

**"balance": 0.00000000,**

"relayfee": 0.00001000,

"warnings": ""

}

И увидим, что несмотря на то, что количество блоков увеличилось – баланс остался нулевым (т.к. майнил только первый узел)

Для того, чтобы делать переводы между кошельками, нам необходим адрес кошелька-получателя. Создадим его.

**Создание публичного адреса кошелька 2**

**tester@d942757991b0 ~/bitcoin-testnet-box$ bitcoin-cli -datadir=2 getnewaddress**

bitcoin-cli -datadir=2 getnewaddress

**bcrt1qzn3yf6wqzfehv2sjrnveewtadzgtfgq2vk9888**

Данная последовательность символов и является адресом созданного кошелька. Попробуем сделать на него перевод с первого кошелька, но сперва донастроим сеть, задав стоимость транзакции (по дефолту она не настроена, а тестовая сеть не дает отработать автонастройке)

**Настройка стоимости транзакции**

**tester@d942757991b0 ~/bitcoin-testnet-box$ bitcoin-cli -datadir=1 settxfee 0.1**

true

Теперь можем переводить средства:

**Перевод средств на полученный адрес**

**tester@d942757991b0 ~/bitcoin-testnet-box$ bitcoin-cli -datadir=1 sendtoaddress "bcrt1qzn3yf6wqzfehv2sjrnveewtadzgtfgq2vk9888" 10**

4dc45a8ff94b352cbe22ed782c87e9a51cb8988a65462697431f439cca081bb5

на выходе получаем ID транзакции.

**Проверяем приход средств**

**tester@d942757991b0 ~/bitcoin-testnet-box$ bitcoin-cli -datadir=1 -getinfo**

bitcoin-cli -datadir=1 -getinfo

{

"version": 210000,

"blocks": 601,

"headers": 601,

"verificationprogress": 1,

"timeoffset": 0,

"connections": {

"in": 1,

"out": 0,

"total": 1

},

"proxy": "",

"difficulty": 4.656542373906925e-10,

"chain": "regtest",

"keypoolsize": 1000,

"paytxfee": 0.10000000,

"balance": 13389.98590000,

"relayfee": 0.00001000,

"warnings": ""

}

**tester@d942757991b0 ~/bitcoin-testnet-box$ bitcoin-cli -datadir=2 -getinfo**

bitcoin-cli -datadir=2 -getinfo

{

"version": 210000,

"blocks": 601,

"headers": 601,

"verificationprogress": 1,

"timeoffset": 0,

"connections": {

"in": 0,

"out": 1,

"total": 1

},

"proxy": "",

"difficulty": 4.656542373906925e-10,

"chain": "regtest",

"keypoolsize": 999,

"paytxfee": 0.00000000,

**"balance": 0.00000000,**

"relayfee": 0.00001000,

"warnings": ""

}

и видим, что ничего не пришло. Почему?

Потому, что транзакция еще не включена в цепочку блоков (не «замайнена»). Надо домайнить блок.

**tester@d942757991b0 ~/bitcoin-testnet-box$ bitcoin-cli -datadir=1 -generate 1**

bitcoin-cli -datadir=1 -generate 1

{

"address": "bcrt1qzt99nkpr574j742rvgl7ksm8gj4jr0f8zhu0t0",

"blocks": [

"5671ad343dd0f0ea18b72e096888e6aef54ecc58c14d99f83a5f8a87080ca130"

]

}

И проверить заново

**tester@d942757991b0 ~/bitcoin-testnet-box$ bitcoin-cli -datadir=1 -getinfo**

bitcoin-cli -datadir=1 -getinfo

{

"version": 210000,

"blocks": 602,

"headers": 602,

"verificationprogress": 1,

"timeoffset": 0,

"connections": {

"in": 1,

"out": 0,

"total": 1

},

"proxy": "",

"difficulty": 4.656542373906925e-10,

"chain": "regtest",

"keypoolsize": 999,

"paytxfee": 0.10000000,

"balance": 13396.23590000,

"relayfee": 0.00001000,

"warnings": ""

}

**tester@d942757991b0 ~/bitcoin-testnet-box$ bitcoin-cli -datadir=2 -getinfo**

bitcoin-cli -datadir=2 -getinfo

{

"version": 210000,

"blocks": 602,

"headers": 602,

"verificationprogress": 1,

"timeoffset": 0,

"connections": {

"in": 0,

"out": 1,

"total": 1

},

"proxy": "",

"difficulty": 4.656542373906925e-10,

"chain": "regtest",

"keypoolsize": 999,

"paytxfee": 0.00000000,

**"balance": 10.00000000**,

"relayfee": 0.00001000,

"warnings": ""

}

Вот теперь средства перешли на кошелек 2. Вы великолепны!