

Лабораторна робота №1

Розгортання локальної bitcoin інфраструктури

Осінній Максим -- ФБ-31мн
Ярошук Владислав -- ФБ-31мн
Золотов Іван -- ФБ-31мп

Локальна інфраструктура складається з 3 трьох компонент:

- Користувачка node user_1
- Користувачка node user_2
- Серверта node яка містить rpc server 'server'

```
Every 2.0s: ss -l | grep 127                                     kali: Wed Apr 10 20:19:50 2024

tcp    LISTEN 0      128                               127.0.0.1:18445              0.0.0.0:*
tcp    LISTEN 0      128                               127.0.0.1:8336              0.0.0.0:*
tcp    LISTEN 0      128                               127.0.0.1:8331              0.0.0.0:*
tcp    LISTEN 0      128                               127.0.0.1:8333              0.0.0.0:*
```

Кожна нода запущена як окремий процес з окремим конфігураційним файлом та під'єднана до rpc серверу

```
2024-04-10T17:27:07Z Opening LevelDB in /home/student/Bitcoin/Labs/server/regtest/chainstate
2024-04-10T17:27:07Z Opened LevelDB successfully
2024-04-10T17:27:07Z Using obfuscation key for /home/student/Bitcoin/Labs/server/regtest/chainstate: 28c51be8362c894b
2024-04-10T17:27:07Z Loaded best chain: hashBestChain=0f9188f13cb7b2c71f2a335e3a4fc328bf5beb436012afca590b1a11466e2206 height=0 date=2011-02-02T23:16:42Z progress=1.000000
2024-04-10T17:27:07Z [snapshot] allocating all cache to the IBD chainstate
2024-04-10T17:27:07Z Opening LevelDB in /home/student/Bitcoin/Labs/server/regtest/chainstate
2024-04-10T17:27:07Z Opened LevelDB successfully
2024-04-10T17:27:07Z Using obfuscation key for /home/student/Bitcoin/Labs/server/regtest/chainstate: 28c51be8362c894b
2024-04-10T17:27:07Z [Chainstate [ibd] @ height 0 (0f9188f13cb7b2c71f2a335e3a4fc328bf5beb436012afca590b1a11466e2206)] resized coinsdb cache to 8.0 MiB
2024-04-10T17:27:07Z [Chainstate [ibd] @ height 0 (0f9188f13cb7b2c71f2a335e3a4fc328bf5beb436012afca590b1a11466e2206)] resized coinstate cache to 440.0 MiB
2024-04-10T17:27:07Z init message: Verifying blocks...
2024-04-10T17:27:07Z block index 72ms

server : bitcoind
2024-04-10T17:27:57Z Setting NODE_NETWORK on non-prune mode
2024-04-10T17:27:57Z block tree size = 1
2024-04-10T17:27:57Z nBestHeight = 0
2024-04-10T17:27:57Z init message: Starting network threads...
2024-04-10T17:27:57Z loadblk thread start
2024-04-10T17:27:57Z Imported mempool transactions from disk: 0 succeeded, 0 failed, 0 expired, 0 already there, 0 waiting for initial broadcast
2024-04-10T17:27:57Z loadblk thread exit
2024-04-10T17:27:57Z net thread start
2024-04-10T17:27:57Z DNS seeding disabled
2024-04-10T17:27:57Z addcon thread start
2024-04-10T17:27:57Z opencon thread start
2024-04-10T17:27:57Z init message: Done loading
2024-04-10T17:27:57Z msghand thread start
2024-04-10T17:27:57Z New outbound peer connected: version: 70016, blocks=0, peer=0 (manual)

server : bitcoind
2024-04-10T17:28:27Z Imported mempool transactions from disk: 0 succeeded, 0 failed, 0 expired, 0 already there, 0 waiting for initial broadcast
2024-04-10T17:28:27Z loadblk thread exit
2024-04-10T17:28:27Z DNS seeding disabled
2024-04-10T17:28:27Z net thread start
2024-04-10T17:28:27Z addcon thread start
2024-04-10T17:28:27Z opencon thread start
2024-04-10T17:28:27Z msghand thread start
2024-04-10T17:28:27Z init message: Done loading
2024-04-10T17:28:27Z New outbound peer connected: version: 70016, blocks=0, peer=0 (manual)
```

Перевірка коннекту до server ноди

```
server : zsh
~/Bitcoin/Labs/server
→ bitcoin-cli -regtest -datadir=$SERVER getconnectioncount
2
```

Для зручності роботи з командною оболонкою створимо псевдоніми на файли конфігурацій для nodes

```
~/Bitcoin/Labs/server  
→ tail -n 6 ~/.zshrc  
  
### LAB CONFIG ###  
export CREDs="-rpcpassword=server -rpcuser=server"  
export SERVER="/home/student/Bitcoin/Labs/server"  
export USER_1="/home/student/Bitcoin/Labs/user_1"  
export USER_2="/home/student/Bitcoin/Labs/user_2"
```

Робота з біткоїн

Для взаємодії з блокчейном користувачі мусять виконати наступні дії:

1. Перевірити статус першого блоку (не обов'язковий крок)
2. Створити гаманець

```

Labs: zsh

→ cd ..

~/Bitcoin/Labs
→ bitcoin-cli -regtest -datadir=$USER_1 createwallet "user_1"
{
  "name": "user_1",
  "warnings": [
    "-fallbackfee is set very high! This is the transaction fee you may pay when fee estimates are not available."
  ],
  "-maxtxfee is set very high! Fees this large could be paid on a single transaction."
}

~/Bitcoin/Labs
→ bitcoin-cli -regtest -datadir=$USER_2 createwallet "user_2"
{
  "name": "user_2",
  "warnings": [
    "-fallbackfee is set very high! This is the transaction fee you may pay when fee estimates are not available."
  ],
  "-maxtxfee is set very high! Fees this large could be paid on a single transaction."
}
}

server: bitcoind — Konsole
File Edit View Bookmarks Plugins Settings Help
main console Labs: zsh server: bitcoind server: http
server: bitcoind

2024-04-10T17:27:07Z Loaded 0 addresses from "anchors.dat"
2024-04-10T17:27:07Z 0 block-relay-only anchors will be tried for connections.
2024-04-10T17:27:07Z init message: Starting network threads.
2024-04-10T17:27:07Z net thread start
2024-04-10T17:27:07Z dnsseed thread start
2024-04-10T17:27:07Z Loading addresses from DNS seed dummySeed.invalid.
2024-04-10T17:27:07Z addcon thread start
2024-04-10T17:27:07Z opencon thread start
2024-04-10T17:27:07Z msghand thread start
2024-04-10T17:27:07Z init message: Done loading
2024-04-10T17:27:07Z 0 addresses found from DNS seeds
2024-04-10T17:27:07Z dnsseed thread exit
2024-04-10T17:28:08Z Adding fixed seeds as 60 seconds have passed and addrman is empty for at least one reachable network
2024-04-10T17:28:08Z Added 0 fixed seeds from reachable networks.

server: bitcoind

2024-04-10T17:32:53Z [user_1] Setting spkMan to active: id = 3ea5e94b060ffbf9e8f6533b4e35171005cf6857aafcd732c8f4b47233aeb768e, type = bech32, internal = false
2024-04-10T17:32:53Z [user_1] Setting spkMan to active: id = ccc94660a21f5ce3da3f5db5af742ebc29c3144e7f42954b3eba9b26c32aetc5, type = bech32m, internal = false
2024-04-10T17:32:53Z [user_1] Setting spkMan to active: id = d19325a79df93bd34ce7f2ef52caadb088afb85ee07077d91c12ace260c67f7, type = legacy, internal = true
2024-04-10T17:32:53Z [user_1] Setting spkMan to active: id = e203333aa06c1d9fb437a2f4c2bea1549c71b062acd210d8c9cc6189f52e8d46, type = p2sh-segwit, internal = true
2024-04-10T17:32:53Z [user_1] Setting spkMan to active: id = d528392d67ce100d9aeb80a4bc22e707f6dcd3c90f18a48d0889808f77e0bb0, type = bech32, internal = true
2024-04-10T17:32:53Z [user_1] Setting spkMan to active: id = 13e83f594ec1c17981251oadfad5027962ff817a103ed39ec71f8f8aad62cc0e, type = bech32m, internal = true
2024-04-10T17:32:53Z [user_1] Wallet completed loading in 1001ms
2024-04-10T17:32:53Z [user_1] setKeyPool.size() = 8000
2024-04-10T17:32:53Z [user_1] mapWallet.size() = 0
2024-04-10T17:32:53Z [user_1] m_address_book.size() = 0

server: bitcoind

2024-04-10T17:33:23Z [user_2] Setting spkMan to active: id = 0aeb446dbebb6ffbf63091a9c489740a685839fc61f020da719b1ab118afe60ad, type = p2sh-segwit, internal = true
2024-04-10T17:33:23Z [user_2] Setting spkMan to active: id = b6f64d32068994c72990abc2a3fd29574e0ed1a543bd22d77fda1d2245420ce, type = bech32, internal = true
2024-04-10T17:33:23Z [user_2] Setting spkMan to active: id = 6fc78a07aafe4920925cc7a81928e1ac7a71eb1880ad665bfe617a0016ee843b, type = bech32m, internal = true
2024-04-10T17:33:23Z [user_2] Wallet completed loading in 1023ms
2024-04-10T17:33:23Z [user_2] setKeyPool.size() = 8000
2024-04-10T17:33:23Z [user_2] mapWallet.size() = 0
2024-04-10T17:33:23Z [user_2] m_address_book.size() = 0
```

3. Визначити йому адресу

```
~/Bitcoin/Labs
→ bitcoin-cli -regtest -datadir=$USER_1 getnewaddress
bcrt1qq8gwqzflz6gnwj6q3zprvs9przq6h6d32c839

~/Bitcoin/Labs
→ bitcoin-cli -regtest -datadir=$USER_2 getnewaddress
bcrt1qeqn69jwkcvgf8vw4awva60ae7hursdjphdjazp
```

4. Намайнити біткоїн

```
Labs : zsh

~/Bitcoin/Labs
→ bitcoin-cli -regtest -datadir=$USER_1 generatetoaddress 101 bcrt1qq8gwqzflz6gnwj
[
  "5f631a78d96c03fb037412684714258a25fc0cd6fbf71b4abe4041e3a20f5bb7",
  "5fdcff9f60091676d4b3b17a1c42739b34ecab5f6ff36ed583510cbb77249fad",
  "6e514761e0963e6c56b95fa02ce70c4c3493f51630fcee367b7fb1e605a496d",
  "41dabc1282989aa2bb022f66b3d735285fe9741ec72b6da9b491554a240fc901",
  "2ce158d14168bdcfa16165cafff97a50605d6cdef1a27a2f54a8df406076d5e6",
  "0505d67a832c3f69c140e36925a39d6ca9792c40a654e9bedc79a00a6528b4d2",
  "5c964be489cc92020a3eb4dae388654a88d8f543ad1d664bc29bd20b9bdbf8dfa",
  "372125cd92756b1c88725d3a299dbbe0e7a720dcaa44d1d0f3415e2bd207c445",
  "4a19e6dff067acad4b7547b75cd3553eb6adb41aaad46cc64f55e0cfa60a6422",
  "09c2184e458e38d86abf307822a1292bb2f6c3489694a380952e2e06e81a6616",
  "5e87e920e6acfd37c564bbe9b4c3fefa7c8fa4362120c6b57861c0af2c032328",
  "3bd0d477c412578adc441aea8c054bc162e7e7116056e8c8e91f49dda7be331b",
  "7cf4449986faa993b760caaf9568e62abf7b2dbf375faab0c4ead924ad5039b",
  "1d9dhaa14d8eed9d5ca7a7083458hd0f2a0c3hfarc123derc050d074hf1fe4d05h62"
]
```

Інформація про блоки розповсюджена поміж нод

```
server : bitcoin — Konsole
File Edit View Bookmarks Plugins Settings Help
main console | Labs : zsh | server : bitcoind | server : http | Labs : zsh |
server : bitcoind

[36:55Z] progress=1.000000 cache=0.0MB(97txo)
2024-04-10T17:13:41Z [net] Saw new header hash=264bfca9e14bd7e7da5d73f93078893efda3e8f84a12c5efff34d2c7b8e03 height=98
2024-04-10T17:13:41Z [net] Saw new capctblock header hash=264bfca9e14bd7e7da5d73f93078893efda3e8f84a12c5efff34d2c7b8e03 peer=0
2024-04-10T17:13:41Z UpdateTip: new best=264bfca9e14bd7e7da5d73f93078893efda3e8f84a12c5efff34d2c7b8e03 height=98 version=0x20000000 log2_work=7.629357 tx=99 date='2024-04-10T17:13:56Z' progress=1.000000 cache=0.0MB(101txo)
2024-04-10T17:13:41Z [net] Saw new header hash=0874ac3ae814ef34b8eba94cc16ee24fba18590a92d751c8caab60df29235 height=99
2024-04-10T17:13:41Z [net] Saw new capctblock header hash=0874ac3ae814ef34b8eba94cc16ee24fba18590a92d751c8caab60df29235 peer=0
2024-04-10T17:13:41Z UpdateTip: new best=0874ac3ae814ef34b8eba94cc16ee24fba18590a92d751c8caab60df29235 height=99 version=0x20000000 log2_work=7.643856 tx=100 date='2024-04-10T17:13:56Z' progress=1.000000 cache=0.0MB(101txo)
2024-04-10T17:13:41Z [net] Saw new capctblock header hash=57b487bae672d12a2a8369f831d8178afa74be87efac13663a5b55abdf82cca height=100
2024-04-10T17:13:41Z [net] Saw new capctblock header hash=57b487bae672d12a2a8369f831d8178afa74be87efac13663a5b55abdf82cca height=100 version=0x20000000 log2_work=7.658211 tx=101 date='2024-04-10T17:13:56Z' progress=1.000000 cache=0.0MB(101txo)
2024-04-10T17:13:41Z [net] Saw new header hash=0de0b23932d83c65d83f693f4f1a1e0ac6918a100d9dd080e0c39fba5cbee height=101
2024-04-10T17:13:41Z [net] Saw new capctblock header hash=0de0b23932d83c65d83f693f4f1a1e0ac6918a100d9dd080e0c39fba5cbee peer=0
2024-04-10T17:13:41Z UpdateTip: new best=0de0b23932d83c65d83f693f4f1a1e0ac6918a100d9dd080e0c39fba5cbee height=101 version=0x20000000 log2_work=7.672425 tx=102 date='2024-04-10T17:13:56Z' progress=1.000000 cache=0.0MB(101txo)
]

server : bitcoind

100 date='2024-04-10T17:13:56Z' progress=1.000000 cache=0.0MB(101txo)
2024-04-10T17:13:41Z CreateNewBlock(): block weight: 888 txs: 0 fees: 0 s!gops 400
2024-04-10T17:13:41Z [net] Saw new header hash=57b487bae672d12a2a8369f831d8178afa74be87efac13663a5b55abdf82cca height=100
2024-04-10T17:13:41Z UpdateTip: new best=57b487bae672d12a2a8369f831d8178afa74be87efac13663a5b55abdf82cca height=100 version=0x20000000 log2_work=7.658211 tx=101 date='2024-04-10T17:13:56Z' progress=1.000000 cache=0.0MB(100txo)
2024-04-10T17:13:41Z CreateNewBlock(): block weight: 888 txs: 0 fees: 0 s!gops 400
2024-04-10T17:13:41Z [net] Saw new header hash=0de0b23932d83c65d83f693f4f1a1e0ac6918a100d9dd080e0c39fba5cbee height=101
2024-04-10T17:13:41Z UpdateTip: new best=0de0b23932d83c65d83f693f4f1a1e0ac6918a100d9dd080e0c39fba5cbee height=101 version=0x20000000 log2_work=7.672425 tx=102 date='2024-04-10T17:13:56Z' progress=1.000000 cache=0.0MB(101txo)
2024-04-10T17:13:41Z [user_] AddToWallet 506fc94e280bf84d776e480c43bb1208fb7ad4fd2e3a447c2cf9105910e454c new
2024-04-10T17:13:41Z [user_] AddToWallet 7db849d6f9e74929fbd8d31de3b79eb72bb5b1f594c50564083f1e36922dc8c new
2024-04-10T17:13:41Z [user_] AddToWallet 73b566a3af2a336f87131ce41c8095eb77d73ed4f1fc67859cd059a878a446 new
2024-04-10T17:13:41Z [user_] AddToWallet 4765d10771e1c0e0c22cbbd3d316de9631a28466c475a79034547363db0b0 new
2024-04-10T17:13:41Z [user_] AddToWallet 5fae157b426cf0a54933d8f6b3606da07c2892340f76eda02e3f01b31 new

server : bitcoind

[36:55Z] progress=1.000000 cache=0.0MB(97txo)
2024-04-10T17:13:41Z [net] Saw new header hash=264bfca9e14bd7e7da5d73f93078893efda3e8f84a12c5efff34d2c7b8e03 height=98
2024-04-10T17:13:41Z [net] Saw new capctblock header hash=264bfca9e14bd7e7da5d73f93078893efda3e8f84a12c5efff34d2c7b8e03 peer=0
2024-04-10T17:13:41Z UpdateTip: new best=264bfca9e14bd7e7da5d73f93078893efda3e8f84a12c5efff34d2c7b8e03 height=98 version=0x20000000 log2_work=7.629357 tx=99 date='2024-04-10T17:13:56Z' progress=1.000000 cache=0.0MB(101txo)
2024-04-10T17:13:41Z [net] Saw new header hash=0874ac3ae814ef34b8eba94cc16ee24fba18590a92d751c8caab60df29235 height=99
2024-04-10T17:13:41Z [net] Saw new capctblock header hash=0874ac3ae814ef34b8eba94cc16ee24fba18590a92d751c8caab60df29235 peer=0
2024-04-10T17:13:41Z UpdateTip: new best=0874ac3ae814ef34b8eba94cc16ee24fba18590a92d751c8caab60df29235 height=99 version=0x20000000 log2_work=7.643856 tx=100 date='2024-04-10T17:13:56Z' progress=1.000000 cache=0.0MB(101txo)
2024-04-10T17:13:41Z [net] Saw new capctblock header hash=57b487bae672d12a2a8369f831d8178afa74be87efac13663a5b55abdf82cca height=100
2024-04-10T17:13:41Z [net] Saw new capctblock header hash=57b487bae672d12a2a8369f831d8178afa74be87efac13663a5b55abdf82cca height=100 version=0x20000000 log2_work=7.658211 tx=101 date='2024-04-10T17:13:56Z' progress=1.000000 cache=0.0MB(101txo)
2024-04-10T17:13:41Z [net] Saw new header hash=0de0b23932d83c65d83f693f4f1a1e0ac6918a100d9dd080e0c39fba5cbee height=101
2024-04-10T17:13:41Z [net] Saw new capctblock header hash=0de0b23932d83c65d83f693f4f1a1e0ac6918a100d9dd080e0c39fba5cbee peer=0
2024-04-10T17:13:41Z UpdateTip: new best=0de0b23932d83c65d83f693f4f1a1e0ac6918a100d9dd080e0c39fba5cbee height=101 version=0x20000000 log2_work=7.672425 tx=102 date='2024-04-10T17:13:56Z' progress=1.000000 cache=0.0MB(101txo)
]
```

~/Bitcoin/Labs

→ `bitcoin-cli -regtest -datadir=$SERVER getblockchaininfo`

```
{
  "chain": "regtest",
  "blocks": 101,
  "headers": 101,
  "bestblockhash": "0de0b239392d833c65d83f693f4f1a1e0ac6918a100d9ddd080e0c3",
  "difficulty": 4.656542373906925e-10,
  "time": 1712770616,
  "mediantime": 1712770615,
  "verificationprogress": 1,
  "initialblockdownload": false,
  "chainwork": "0000000000000000000000000000000000000000000000000000000000000000",
  "size_on_disk": 30375,
  "pruned": false,
  "warnings": ""
}
```

○

5. Провести транзакцію

- Після створення 101 блоку на рахунку user_1 50 біткоїнів А.

```
→ bitcoin-cli -regtest -datadir=$SERVER getbalance
error code: -18
error message:
No wallet is loaded. Load a wallet using loadwallet or
  (if -wallet is no longer automatically created)

~/Bitcoin/Labs
→ bitcoin-cli -regtest -datadir=$USER_1 getbalance
50.00000000

~/Bitcoin/Labs
→ bitcoin-cli -regtest -datadir=$USER_2 getbalance
0.00000000
```

- Переведемо 25 біткоїнів користувачу user_2

```
~/Bitcoin/Labs
→ bitcoin-cli -regtest -datadir=$USER_1 sendtoaddress bcr1t1eqn69jwkcvgf8vw4awva60ae7hursdjphdjazp
437e7db6676fb5f7ab44677c87c06062113b6122245c6a861e7cd8d5158cbeed

~/Bitcoin/Labs
→ bitcoin-cli -regtest -datadir=$USER_2 getbalance
0.00000000

~/Bitcoin/Labs
→ bitcoin-cli -regtest -datadir=$USER_1 getbalance
24.85900000

~/Bitcoin/Labs
→
```

- Переглянемо транзакцію так як кошти знялися але не відображаються для **\$USER_2**

[illegible]

- Дебаг показав що наші ноди не бачать одна одну, але сервер бачить їх обох

A.

- A.

}