USE IT

BITCOIN SIMULATOR

The Bitcoin Simulator can be easily configured via command line parameters. Below is presented a table of all the input parameters along with their default values.

INPUT PARAMETERS

Parameter	Description	Default Value
blockSize	The fixed block size (Bytes). If the default value is used then the blockSize follows the real bitcoin block size distribution as estimated by collecting stats from blockchain.info	-1
noBlocks	The number of generated blocks	100
nodes	The total number of nodes in the network. The number of nodes should always be greater of equal to the number of miners. The number of miners, their hash rates and their locations can be changed by modifying the variables **bitcoinMinersHash/litecoinMinersHash/dogecoinMinersHash** and **bitcoinMinersRegions/litecoinMinersRegions/dogecoinMinersRegions**.	16
minConnections	The minConnectionsPerNode of the grid.	-1
maxConnections	The maxConnectionsPerNode of the grid. If minConnections <= 0 or maxConnections <=0, the nodes follow the connections distribution as described in here.	-1
blockIntervalMinutes	The average block generation interval in minutes.	10
invTimeoutMins	The inv block timeout. If the default value is used, the timeouts are twice as long as blockIntervalMinutes.	-1
unsolicited	Change the miners block broadcast type to UNSOLICITED. Each newly mined block is broadcast immediately to all the peers of the miner who mined it.	false
relayNetwork	Change the miners block broadcast type to RELAY_NETWORK. The miners use a relay network for communicating among themselves and send compressed blocks.	false
unsolicitedRelayNetwork	Change the miners block broadcast type to UNSOLICITED_RELAY_NETWORK. The miners use a relay network among themselves and send compressed blocks and each newly mined block is broadcast immediately to all the peers of the miner who mined it.	false
sendheaders	Change the protocol to sendheaders.	false
litecoin	Imitate the litecoin network behaviour. It sets the --nodes=1000, --blockIntervalMinutes=2.5, follows the same connection distribution as bitcoin, but the litecoin distribution for the block generation interval and block size.	false
dogecoin	Imitate the dogecoin network behaviour. It sets the --nodes=650, --blockIntervalMinutes=1, follows the same connection distribution as bitcoin, but the dogecoin distribution for the block generation interval and block size.	false
blockTorrent	Enable the BlockTorrent protocol.	false
chunkSize	The chunksize of the blockTorrent in Bytes. Used only in conjuction with --blockTorrent.	-1
spv	Enable the spv mechanism in blockTorrent.Used only in conjuction with --blockTorrent. The nodes are able to advertise chunks of blocks which are not yet validated.	false

OPTIMAL ADVERSARIAL ATTACKER

The optimal adversarial attacker can also be configured via command line parameters. Below is presented a table of all the input parameters along with their default values.

INPUT PARAMETERS

Parameter	Description	Default Value
blockIntervalMinutes	The average block generation interval in minutes.	10
noBlocks	The number of generated blocks	100
ud	The transaction value which is double-spent. If ud = 0, the attacker follows the optimal strategy for selfish-mining. Otherwise, the attacker follows the optimal strategy for performing a double-spending attack of a transaction with value equals to ud.	0
r	The stale block rate	0
unsolicited	Change the miners block broadcast type to UNSOLICITED. Each newly mined block is broadcast immediately to all the peers of the miner who mined it.	false
relayNetwork	Change the miners block broadcast type to RELAY_NETWORK. The miners use a relay network for communicating among themselves and send compressed blocks.	false
unsolicitedRelayNetwork	Change the miners block broadcast type to UNSOLICITED_RELAY_NETWORK. The miners use a relay network among themselves and send compressed blocks and each newly mined block is broadcast immediately to all the peers of the miner who mined it.	false

Notes

- The number of miners, their hash rates and their locations can be changed by modifying the arrays ***minersHash*** and ***minersRegions***. The attacker's hash rate is always the last value in ***minersHash***.
- To modify the optimal strategy, the ***m_decisionMatrix*** in ***bitcoin-selfish-miner.h*** must be updated accordingly.

TUTORIAL

Here we demonstrate some basic examples of how you can use the simulator:

- If you want to run a simple Bitcoin simulation for 100 blocks and 6000 nodes, you can just enter the following command:

```
./waf --run "bitcoin-test --noBlocks=100 --nodes=6000"
```

- If you want to start the simulation for 1000 blocks in LITECOIN mode and with a block size of 2MB you have to enter the following command:

```
./waf --run "bitcoin-test --noBlocks=1000 --litecoin --blockSize=2000000"
```

- You can also use **mpi** to speed up the simulation:

```
mpirun -n 2 ./waf --run "bitcoin-test --noBlocks=1000 --litecoin --blockSize=2000000"
```