CS554 Project #2

Blockchain Simulation

Instructions:

- *Assigned date: Saturday June 14th, 2025*
- *Due date: 11:59PM on Friday June 27th, 2025*
- *Maximum Points: 150; +50 for Extra Credit Points*
- *This assignment must be done individually*
- *Please post questions to professor by email*
- *Only a softcopy submission is required through Canvas*
- *Late submission will be penalized at 20% per day*

1 Your Assignment

In this assignment, you will build a discrete-event simulation of a simplified blockchain network using the Python SimPy framework (pip3 install simpy). You will model nodes, transaction pools, miners, difficulty adjustment, and coin issuance. By completing this exercise, you will practice:

- Designing event-driven simulations with SimPy processes and events
- Managing global state (network metrics, transaction pool, coin balances)
- Implementing Poisson/exponential arrival processes (mining & wallet txs)
- Writing modular, CLI-driven Python programs
- Applying difficulty-retarget logic and halving schedules
- Verifying correctness via summary statistics (block time, TPS, coin supply)

2 Assignment Requirements

Write a Python script named sim-blockchain.py that implements the following features. Command-line arguments must match the descriptions below.

2.1 Network & Blocks

1. **Nodes** (--nodes N): Create N peer nodes, each maintaining a set of stored block IDs. Randomly connect each node to --neighbors M distinct peers.
2. **Block structure**: Each block has a header (1,024 bytes) + (# transactions × 256 bytes). Track block ID, timestamp, time-since-last-block, transaction count, and size.
3. **Block propagation**: When a node stores a new block, it broadcasts it to neighbors (increment a global io_requests counter per send; add block size to network_data). Ignore duplicates.

2.2 Mining & Difficulty

1. **Miners** (--miners K, --hashrate H): Spawn K miner processes, each with hashrate H. Expected time per block ~ Exp(total_hashrate / difficulty).

2. **Difficulty** (--blocktime T, --difficulty D optional): If D not set, initialize to T × (K × H). After every 2,016 blocks, retarget:

   new_diff = old_diff × (target_blocktime / actual_avg_blocktime)

3. **Halving & coin issuance** (--reward R, default 50): Issue R coins per block. Every --halving H blocks (default 210000), halve the reward; after 35 halvings, reward → 0.

2.3 Transactions & Wallets

1. **Wallets** (--wallets W, --transactions X, --interval I): Generate W wallet processes; each sends X transactions into a global unconfirmed-pool at interval I seconds.
2. **Block filling**: On block creation, include up to --blocksize B transactions from the pool (FIFO), plus the mining reward transaction.
3. **Termination**:
   - If --blocks L is specified, run until **L** blocks have been mined or until all txs are processed (whichever comes first).
   - If --blocks omitted, run until all wallet transactions have been confirmed.

2.4 Reporting & CLI Options

- --print P (default 144): Print a summary every P blocks; with --debug, print every block. Summaries must include:

  [time] Sum B:blocks/totalBlocks complete% abt:avg_block_time(s) tps:confirmed_tx_per_sec infl:inflation% ETA:seconds Diff:xx Hash:xx Tx:total_tx C:coins Pool:pending_tx NMB:network_MB IO:io_requests

- Final summary:
  [******] End B:blocks abt:avg_block_time(s) tps:confirmed_tx_per_sec Tx:total_tx C:coins NMB:network_MB IO:io_requests

2.5 Workloads to evaluate

Run BTC, BCH, LTC, DOGE, and MEMO for 10 years with no user transactions, and report the number of coins created and simulation time taken. See the details for each blockchain in the table below. Some of these simulations might take a lot of time, potentially tens of minutes for each simulation, depending on how you implemented it. Since your simulation is not multi-threaded, you can run multiple simulations at the same time for different configurations as long as you have a dedicated CPU core per simulation process. Then run BTC, BCH, LTC, DOGE, and MEMO with a small, medium, and large workload of transactions.

- SMALL: 10 wallets with 10 transactions each generated with interval of 10.0
- MEDIUM: 1000 wallets with 1000 transactions each generated with interval of 1.0
- LARGE: 1000 wallets with 1000 transactions each generated with interval of 0.01

Chain	Block Reward	Halving Schedule	Block Time	Block Size Limit	Max TX per Block
Bitcoin (BTC)	50 BTC	210K blocks	600 sec	1 MB base	4K TX
Bitcoin Cash (BCH)	12.5 BCH	210K blocks	600 sec	32 MB	128K TX
Litecoin (LTC)	50 LTC	840K blocks	150 sec	1 MB	4K TX
Dogecoin (DOGE)	10 000 DOGE (static)	None	60 sec	1 MB	4K TX
MEMO	51.8457072 MEMO	9644K blocks	3.27 sec	8 MB	32K TX

2.5 Sample Output

```
(venv) (base) dhcp26:proj2 iraicu$ time python3 sim-blockchain2.py --miners 2 --hashrate 1e6 --nodes 2 --neighbors 1 --blocktime 100 --blocksize 1000 --wallets 1000 --transactions 250 --interval 10.0 --print 10 --reward 1000 --halving 10000 --years 1

[1266.11] Sum B:10/315360 0.0% abt:126.61s tps:7.91 infl:0.00% ETA:39926642.68s Diff:200M H:2M Tx:10010 C:10K Pool:116000 NMB:4.63 IO:18
[3135.94] Sum B:20/315360 0.0% abt:186.98s tps:5.35 infl:1686567.25% ETA:58963330.79s Diff:200M H:2M Tx:20020 C:20K Pool:230000 NMB:9.78 IO:38
[3781.77] Sum B:30/315360 0.0% abt:64.58s tps:15.50 infl:2441493.75% ETA:20365087.69s Diff:200M H:2M Tx:30030 C:30K Pool:220000 NMB:14.92 IO:58
[4479.74] Sum B:40/315360 0.0% abt:69.80s tps:14.34 infl:1506094.00% ETA:22008213.51s Diff:200M H:2M Tx:40040 C:40K Pool:210000 NMB:20.07 IO:78
[4906.67] Sum B:50/315360 0.0% abt:42.69s tps:23.45 infl:1846676.81% ETA:13461500.28s Diff:200M H:2M Tx:50050 C:50K Pool:200000 NMB:25.21 IO:98
[5726.54] Sum B:60/315360 0.0% abt:81.99s tps:12.21 infl:769288.22% ETA:25850651.42s Diff:200M H:2M Tx:60060 C:60K Pool:190000 NMB:30.36 IO:118
[6614.86] Sum B:70/315360 0.0% abt:88.83s tps:11.27 infl:591682.66% ETA:28007652.75s Diff:200M H:2M Tx:70070 C:70K Pool:180000 NMB:35.50 IO:138
[7425.16] Sum B:80/315360 0.0% abt:81.03s tps:12.35 infl:555980.69% ETA:25547316.18s Diff:200M H:2M Tx:80080 C:80K Pool:170000 NMB:40.65 IO:158
[8355.07] Sum B:90/315360 0.0% abt:92.99s tps:10.76 infl:423912.46% ETA:29317240.43s Diff:200M H:2M Tx:90090 C:90K Pool:160000 NMB:45.80 IO:178
[9664.29] Sum B:100/315360 0.0% abt:130.92s tps:7.65 infl:267641.12% ETA:41274339.48s Diff:200M H:2M Tx:100100 C:100K Pool:150000 NMB:50.94 IO:198
[10887.29] Sum B:110/315360 0.0% abt:122.30s tps:8.18 infl:257857.78% ETA:38555067.78s Diff:200M H:2M Tx:110110 C:110K Pool:140000 NMB:56.09 IO:218
[11964.51] Sum B:120/315360 0.0% abt:107.72s tps:9.29 infl:266139.06% ETA:33958353.19s Diff:200M H:2M Tx:120120 C:120K Pool:130000 NMB:61.23 IO:238
[12959.54] Sum B:130/315360 0.0% abt:99.50s tps:10.06 infl:264112.54% ETA:31366342.96s Diff:200M H:2M Tx:130130 C:130K Pool:120000 NMB:66.38 IO:258
[14042.22] Sum B:140/315360 0.0% abt:108.27s tps:9.25 infl:224059.96% ETA:34128152.11s Diff:200M H:2M Tx:140140 C:140K Pool:110000 NMB:71.52 IO:278
[14755.04] Sum B:150/315360 0.0% abt:71.28s tps:14.04 infl:316005.50% ETA:22469009.18s Diff:200M H:2M Tx:150150 C:150K Pool:100000 NMB:76.67 IO:298
[16009.32] Sum B:160/315360 0.1% abt:125.43s tps:7.98 infl:167618.95% ETA:39534699.37s Diff:200M H:2M Tx:160160 C:160K Pool:90000 NMB:81.82 IO:318
[16542.53] Sum B:170/315360 0.1% abt:53.32s tps:18.77 infl:369646.88% ETA:16806296.13s Diff:200M H:2M Tx:170170 C:170K Pool:80000 NMB:86.96 IO:338
[17690.16] Sum B:180/315360 0.1% abt:114.76s tps:8.72 infl:161642.89% ETA:36170933.71s Diff:200M H:2M Tx:180180 C:180K Pool:70000 NMB:92.11 IO:358
[18845.65] Sum B:190/315360 0.1% abt:115.55s tps:8.66 infl:151623.00% ETA:36417815.92s Diff:200M H:2M Tx:190190 C:190K Pool:60000 NMB:97.25 IO:378
[20095.01] Sum B:200/315360 0.1% abt:124.94s tps:8.01 infl:132851.76% ETA:39374657.81s Diff:200M H:2M Tx:200200 C:200K Pool:50000 NMB:102.40 IO:398
[20829.13] Sum B:210/315360 0.1% abt:73.41s tps:13.64 infl:214788.13% ETA:23135753.62s Diff:200M H:2M Tx:210210 C:210K Pool:40000 NMB:107.54 IO:418
[21205.79] Sum B:220/315360 0.1% abt:37.67s tps:26.58 infl:398687.97% ETA:11870191.06s Diff:200M H:2M Tx:220220 C:220K Pool:30000 NMB:112.69 IO:438
[22064.04] Sum B:230/315360 0.1% abt:85.82s tps:11.66 infl:167021.61% ETA:27045872.79s Diff:200M H:2M Tx:230230 C:230K Pool:20000 NMB:117.83 IO:458
[23063.08] Sum B:240/315360 0.1% abt:99.90s tps:10.02 infl:137243.72% ETA:31481995.96s Diff:200M H:2M Tx:240240 C:240K Pool:10000 NMB:122.98 IO:478
[24284.73] Sum B:250/315360 0.1% abt:122.16s tps:8.19 infl:107559.82% ETA:38495280.37s Diff:200M H:2M Tx:250250 C:250K Pool:0 NMB:128.13 IO:498
[******] End B:250/315360 100.0% abt:97.14s tps:10.30 infl:0.00% Diff:200M H:2M Tx:250250 C:250K Pool:0 NMB:128.13 IO:498

real    0m5.477s
user    0m5.420s
sys     0m0.023s

(venv) (base) dhcp26:proj2 iraicu$ time python3 sim-blockchain2.py --miners 2 --hashrate 1e6 --nodes 2 --neighbors 1 --blocktime 100 --blocksize 1000 --wallets 1 --transactions 0 --interval 10.0 --print 10000 --reward 1000 --halving 10000 --years 1 > log1.txt

[998104.14] Sum B:10000/315360 3.2% abt:99.81s tps:0.01 infl:0.00% ETA:30478108.04s Diff:202.7M H:2M Tx:10000 C:10M Pool:0 NMB:25.60 IO:19998
[1997298.11] Sum B:20000/315360 6.3% abt:99.92s tps:0.01 infl:1578.07% ETA:29512193.01s Diff:197.5M H:2M Tx:20000 C:15M Pool:0 NMB:51.20 IO:39998
[3000721.11] Sum B:30000/315360 9.5% abt:100.34s tps:0.01 infl:523.81% ETA:28633678.83s Diff:194.3M H:2M Tx:30000 C:17.5M Pool:0 NMB:76.80 IO:59998
[4007069.23] Sum B:40000/315360 12.7% abt:100.63s tps:0.01 infl:223.84% ETA:27710801.93s Diff:196.1M H:2M Tx:40000 C:18.8M Pool:0 NMB:102.40 IO:79998
[5003227.85] Sum B:50000/315360 15.9% abt:99.62s tps:0.01 infl:105.53% ETA:26434065.13s Diff:200.1M H:2M Tx:50000 C:19.4M Pool:0 NMB:128.00 IO:99998
[5994327.75] Sum B:60000/315360 19.0% abt:99.11s tps:0.01 infl:51.32% ETA:25308726.92s Diff:206.0M H:2M Tx:60000 C:19.7M Pool:0 NMB:153.60 IO:119998
[7003683.53] Sum B:70000/315360 22.2% abt:100.94s tps:0.01 infl:24.80% ETA:24765553.31s Diff:202.5M H:2M Tx:70000 C:19.8M Pool:0 NMB:179.20 IO:139998
[8010915.49] Sum B:80000/315360 25.4% abt:100.72s tps:0.01 infl:12.33% ETA:23706211.42s Diff:201.6M H:2M Tx:80000 C:19.9M Pool:0 NMB:204.80 IO:159998
[9004368.90] Sum B:90000/315360 28.5% abt:99.35s tps:0.01 infl:6.22% ETA:22388466.25s Diff:204.9M H:2M Tx:90000 C:20.0M Pool:0 NMB:230.40 IO:179998
[10008565.75] Sum B:100000/315360 31.7% abt:100.42s tps:0.01 infl:3.07% ETA:21626383.31s Diff:193.0M H:2M Tx:100000 C:20.0M Pool:0 NMB:256.00 IO:199998
[11012774.41] Sum B:110000/315360 34.9% abt:100.42s tps:0.01 infl:1.53% ETA:20622428.98s Diff:204.0M H:2M Tx:110000 C:20.0M Pool:0 NMB:281.60 IO:219998
[12001660.70] Sum B:120000/315360 38.1% abt:98.89s tps:0.01 infl:0.78% ETA:19318882.62s Diff:212.5M H:2M Tx:120000 C:20.0M Pool:0 NMB:307.20 IO:239998
[13011736.45] Sum B:130000/315360 41.2% abt:101.01s tps:0.01 infl:0.38% ETA:18722764.02s Diff:199.0M H:2M Tx:130000 C:20.0M Pool:0 NMB:332.80 IO:259998
[14014698.79] Sum B:140000/315360 44.4% abt:100.30s tps:0.01 infl:0.19% ETA:17587947.60s Diff:190.3M H:2M Tx:140000 C:20.0M Pool:0 NMB:358.40 IO:279998
[15019137.87] Sum B:150000/315360 47.6% abt:100.44s tps:0.01 infl:0.10% ETA:16609404.62s Diff:191.0M H:2M Tx:150000 C:20.0M Pool:0 NMB:384.00 IO:299998
[16014416.67] Sum B:160000/315360 50.7% abt:99.53s tps:0.01 infl:0.05% ETA:15462651.52s Diff:195.1M H:2M Tx:160000 C:20.0M Pool:0 NMB:409.60 IO:319998
[17010766.50] Sum B:170000/315360 53.9% abt:99.63s tps:0.01 infl:0.02% ETA:14482941.07s Diff:208.2M H:2M Tx:170000 C:20.0M Pool:0 NMB:435.20 IO:339998
[18006921.77] Sum B:180000/315360 57.1% abt:99.62s tps:0.01 infl:0.01% ETA:13483957.78s Diff:203.6M H:2M Tx:180000 C:20.0M Pool:0 NMB:460.80 IO:359998
[19015345.82] Sum B:190000/315360 60.2% abt:100.84s tps:0.01 infl:0.01% ETA:12641603.91s Diff:197.6M H:2M Tx:190000 C:20.0M Pool:0 NMB:486.40 IO:379998
[20007098.08] Sum B:200000/315360 63.4% abt:99.18s tps:0.01 infl:0.00% ETA:11440854.08s Diff:205.1M H:2M Tx:200000 C:20.0M Pool:0 NMB:512.00 IO:399998
[21009798.78] Sum B:210000/315360 66.6% abt:100.27s tps:0.01 infl:0.00% ETA:10564454.57s Diff:203.9M H:2M Tx:210000 C:20.0M Pool:0 NMB:537.60 IO:419998
[22019577.73] Sum B:220000/315360 69.8% abt:100.98s tps:0.01 infl:0.00% ETA:9629252.01s Diff:197.0M H:2M Tx:220000 C:20.0M Pool:0 NMB:563.20 IO:439998
[23018227.43] Sum B:230000/315360 72.9% abt:99.86s tps:0.01 infl:0.00% ETA:8524473.87s Diff:198.6M H:2M Tx:230000 C:20.0M Pool:0 NMB:588.80 IO:459998
[24022865.14] Sum B:240000/315360 76.1% abt:100.46s tps:0.01 infl:0.00% ETA:7570949.75s Diff:194.3M H:2M Tx:240000 C:20.0M Pool:0 NMB:614.40 IO:479998
[25018434.80] Sum B:250000/315360 79.3% abt:99.56s tps:0.01 infl:0.00% ETA:6507043.31s Diff:200.1M H:2M Tx:250000 C:20.0M Pool:0 NMB:640.00 IO:499998
[26019545.48] Sum B:260000/315360 82.4% abt:100.11s tps:0.01 infl:0.00% ETA:5542148.73s Diff:199.4M H:2M Tx:260000 C:20.0M Pool:0 NMB:665.60 IO:519998
[27019118.98] Sum B:270000/315360 85.6% abt:99.96s tps:0.01 infl:0.00% ETA:4534065.38s Diff:195.4M H:2M Tx:270000 C:20.0M Pool:0 NMB:691.20 IO:539998
[28014647.03] Sum B:280000/315360 88.8% abt:99.55s tps:0.01 infl:0.00% ETA:3520187.21s Diff:199.9M H:2M Tx:280000 C:20.0M Pool:0 NMB:716.80 IO:559998
[29020495.35] Sum B:290000/315360 92.0% abt:100.58s tps:0.01 infl:0.00% ETA:2550831.34s Diff:198.5M H:2M Tx:290000 C:20.0M Pool:0 NMB:742.40 IO:579998
[30016881.51] Sum B:300000/315360 95.1% abt:99.64s tps:0.01 infl:0.00% ETA:1530449.14s Diff:203.3M H:2M Tx:300000 C:20.0M Pool:0 NMB:768.00 IO:599998
[31026185.35] Sum B:310000/315360 98.3% abt:100.93s tps:0.01 infl:0.00% ETA:540986.86s Diff:198.0M H:2M Tx:310000 C:20.0M Pool:0 NMB:793.60 IO:619998
[******] End B:315360/315360 100.0% abt:100.07s tps:0.01 infl:0.00% Diff:205.4M H:2M Tx:315360 C:20.0M Pool:0 NMB:807.32 IO:630718

real    0m5.968s
user    0m5.929s
sys     0m0.027s
```

2.6 Extra Credit

- Simulate network latency by adding delays on receive broadcasts; ensure that block propagation happens within the blocktime
- Simulate network bandwidth by taking into account block size; simulating larger block sizes should take longer to propagate
- Track per-wallet balances and include fee logic
- Allow simulator to load traces from real world, such as transactions, miners joining and leaving to mimic global hashrate, etc

3 What you will submit

You should hand in:

1. **Source code:** All of the source code, including proper documentation and formatting.
2. **Readme:** A detailed manual describing the structure of your files and directory organization. The manual should be able to instruct users how to run the program step by step. The manual should contain example commands. This should be included as readme.txt in the source code folder.
3. **Report:** A written document (typed, named report.pdf) describing the overall assignment completion, along with screen shots of sample output. Make sure to include your results for various runs in a table.

You will put everything outlined above in a folder called “proj2-lastname” and compress it with ZIP or TAR utilities.

4 Where you will submit

You will have to submit your final compressed archive through Canvas.
Grades for late submissions will be lowered 20% per day late.