Simulation of a P2P Cryptocurrency Network

CS 765 - Introduction of Blockchains, Cryptocurrencies, and Smart Contracts

Spring 2024

Indian Institute of Technology Bombay

Authors:

Debdoot (23M0765)

Nilava Sarkar (22M0753)

Niraj Jaiswal (22M0779)

Lecturer:

Prof. Vinay Joseph Ribeiro

Dept. of CSE, IIT Bombay

February 19, 2024

1. Introduction

We've developed a discrete-event simulator tailored for a peer-to-peer cryptocurrency network. This type of simulator operates by managing an event queue alongside a global clock. It selects and processes the earliest event from this queue and may generate additional events based on the execution outcome. In our report, we detail various design decisions and conduct analyses on diverse simulations utilizing different system parameters outlined in the configuration file.

2. What are the theoretical reasons of choosing the exponential distribution?

The exponential distribution is chosen because it assumes transaction arrivals are random and independent, consistent with real-world behavior. It's mathematically simple and aligns with the Poisson process, making analysis easier. Empirical data also supports its use.

Let Δ be the small time interval and probability of mining a block in time Δ be $\beta\Delta$, where β depends on the hashing power. Let $I(I = n\Delta)$ be the time interval. The probability of mining a block is time interval I can be drawn from an exponential distribution with mean $\frac{1}{\beta}$ show in below equations.

$P[I = n\Delta] = (1 - \beta\Delta)^{n-1}\beta\Delta$

$P[I > n\Delta] = (1 - \beta\Delta)^{n}$

let $n\Delta = x$

$P[I > x] = (1 - \frac{\beta\Delta}{n})^{n}$

when $n \to \infty$ the geometric distribution behaves like exponential distribution.

$$P[I > x] = e^{-\beta x}$$

3. Why is the mean of d_{ij} inversely related to c_{ij}? Give justification for this choice.

When the link speed of a node, denoted as c_{ij}, is high, the time needed to buffer packets in the queue decreases. Consequently, packets spend less time waiting in the queue, resulting in a reduction in the average queuing delay, d_{ij}.

4. Reason for choosing a particular mean T_k to get the random block generation time from exponential distribution?

A small T_k leads to a high frequency of block generation, increasing the likelihood of forks and decreasing the number of transactions per block. Conversely, a very large T_k reduces fork occurrences but may result in fewer blocks generated, leading to transaction backlog in the pending transaction pool. Therefore, finding a balanced T_k is crucial, considering its impact on forks and transaction volume per block.

5. Flowchart

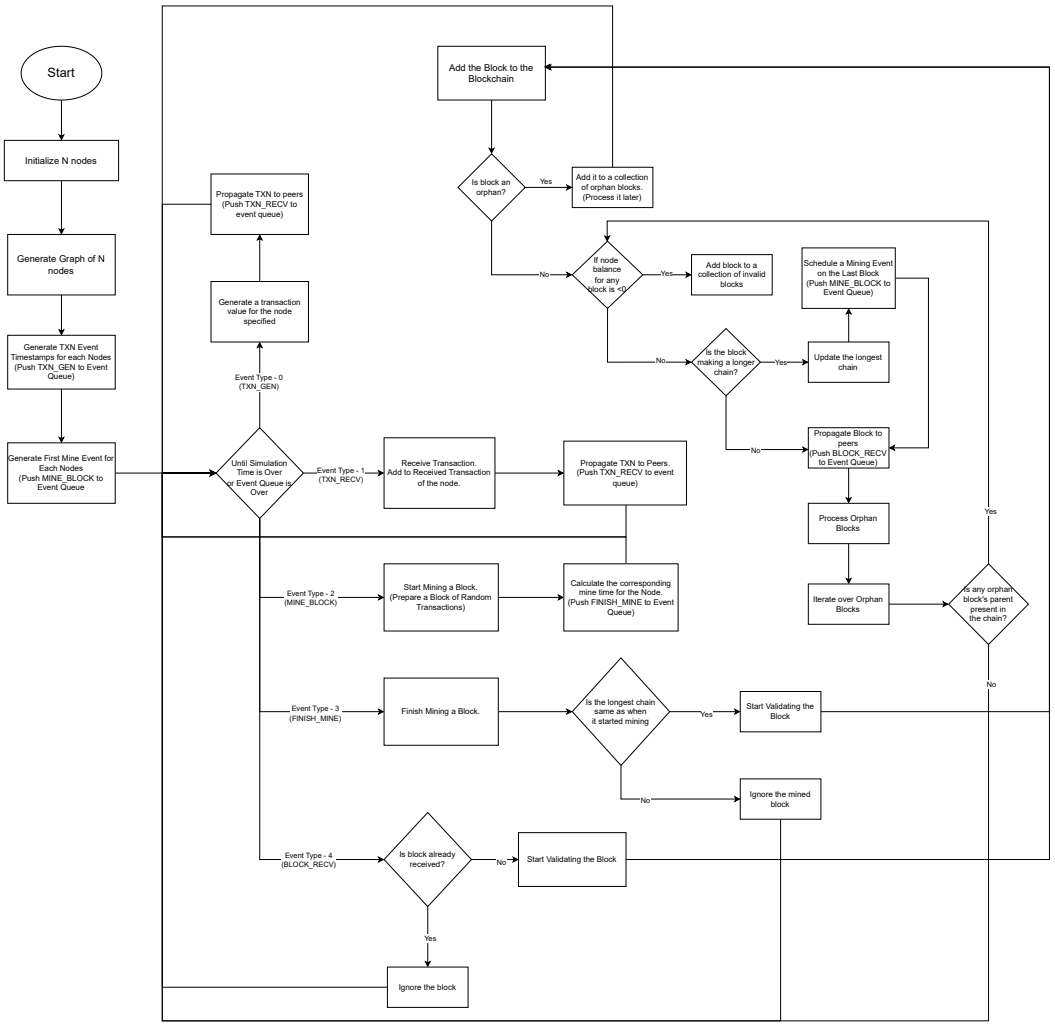

Figure 1: Event Flow Diagram

6. Observation

Data for the two experiments performed is given below:

Simulation Time (60000 sec), interarrival time for Block (500 sec) and Transaction (10 sec) is kept constant.

6.1 z0 (Low Speed) - 20% and z1 (Low CPU) - 80%

Node Number	Hashing Power	Speed	#Blocks in Chain	#Blocks in Longest Chain	Block Mined	Block in Chain
0	Low	High	136	136	1	1
1	High	High	136	136	39	39
2	Low	Low	136	136	7	7
3	Low	High	136	136	8	8
4	Low	High	136	136	3	3
5	High	High	136	136	58	58
6	Low	High	136	136	4	4
7	Low	High	136	136	5	5
8	Low	Low	136	136	5	5
9	Low	High	136	136	5	5

Blockchain tree for the above experiment is attached below:

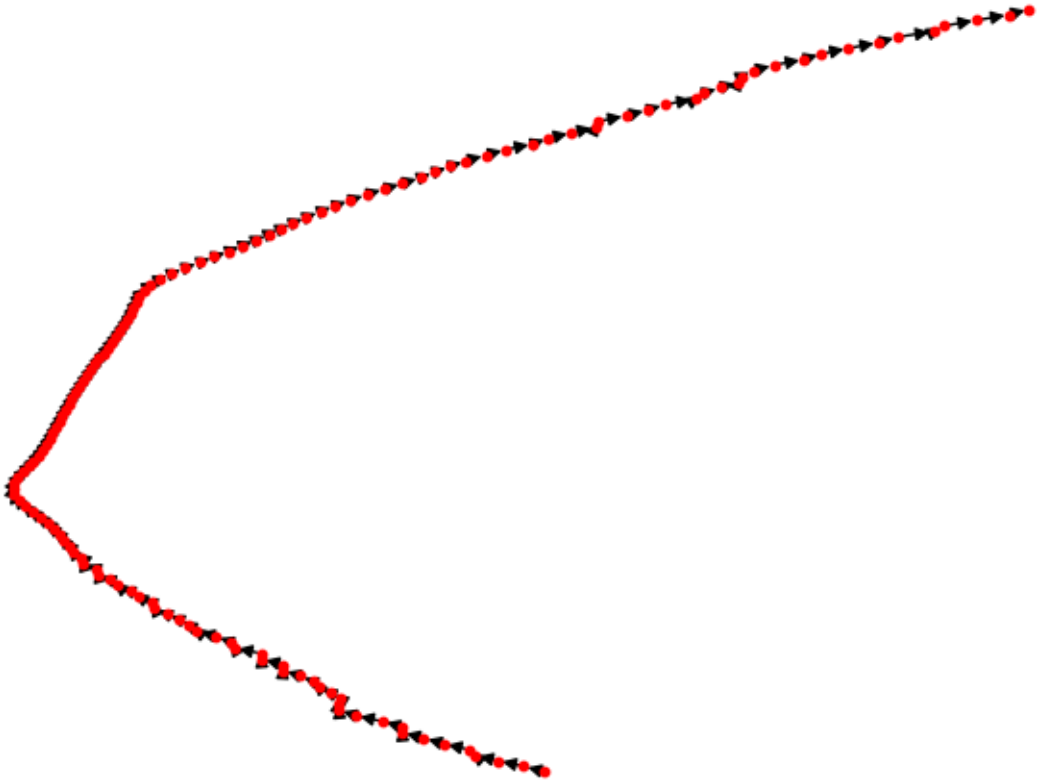

Figure 2: Blockchain Tree1

Obs1 - "With less high powered CPU Nodes and more high speed Nodes, blocks will be propagated more faster than it's generation. Hence almost no chance of fork given the interarrival time of blocks 600s. There could be forks if interarrival time for block is set lower in the given condition of z0 and z1."

6.2 z0 (Low Speed) - 80% and z1 (Low CPU) - 20%

Node Number	Hashing Power	Speed	#Blocks in Chain	#Blocks in Longest Chain	Block Mined	Block in Chain
0	High	Low	128	125	15	14
1	High	Low	128	125	21	20
2	High	Low	128	125	6	6
3	High	Low	128	125	21	20
4	High	Low	128	125	20	20
5	High	Low	128	125	17	17
6	High	Low	128	125	12	12
7	High	High	128	125	12	12
8	Low	Low	128	125	2	2
9	Low	High	128	125	2	2

Blockchain tree for the above experiment is attached below:

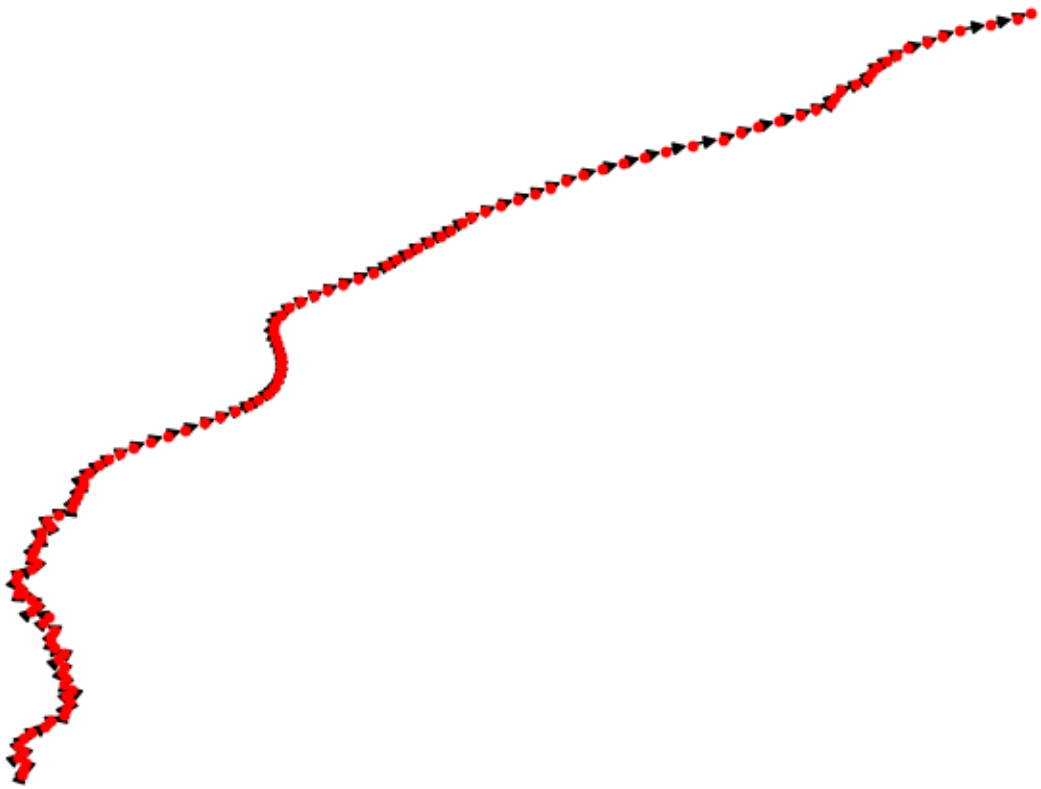

Figure 3: Blockchain Tree2

Obs2 - "With more high powered CPU Nodes and less high speed Nodes, blocks will be propagated slower than it's generation. Hence more chance of fork." Obs2 - "With more high powered CPU Nodes and less high speed Nodes, blocks will be propagated slower than it's generation. Hence more chances of fork given the interarrival time of blocks 600s. There could be more forks if interarrival time for block is set lower in the given condition of z0 and z1."

7. Conclusion

- The high powered nodes mined more blocks (almost 10 times) than the low powered nodes. So, the contribution of high powered nodes is more than the low powered nodes in the longest chain.
- Higher the value of z_0 (number of nodes with low speed), the slower the blocks will propagate, hence creating more chances for forks.
- Higher the value of z_1 (number of nodes with low CPU), the slower the block generation, hence creating fewer chances for forks.
- Lower the interarrival time of blocks, higher is the chance of forking as blocks will be generated faster than the propagation. Hence creating more number of blocks.