A Report on Assignment 1
of
Simulation of a P2P Cryptocurrency Network

Introduction of Blockchains, Cryptocurrencies, and Smart Contracts

CS 765

Created By

Santanu Sahoo (23M0777)
Arnab Bhakta (23M0835)

IIT Bombay
Mumbai

Instructor

Prof. Vinay Ribeiro

Contents

1 Introduction **2**

2 Background **3**

3 Theoretical proofs **4**

4 Visualization and Analysis **6**
4.1 Analysis of first Simulation 6
4.1.1 Experiment Parameters: 6
4.1.2 Results: 6
4.1.3 Statistics 7
4.1.4 Blockchain Tree 8
4.2 Analysis of Second Simulation 9
4.2.1 Experiment Parameters: 9
4.2.2 Results: 9
4.2.3 Statistics 10
4.2.4 Blockchain Tree 12
4.3 Analysis of Third Simulation 13
4.3.1 Experiment Parameters: 13
4.3.2 Results: 13
4.3.3 Statistics 14
4.3.4 Blockchain Tree 16
4.4 Analysis of fourth Simulation 17
4.4.1 Experiment Parameters: 17
4.4.2 Results: 17
4.4.3 Statistics 18
4.4.4 Blockchain Tree 19

5 References **20**

1 Introduction

Cryptocurrencies have sparked a revolution in finance, offering an alternative to traditional centralized banking systems. With the advent of Bitcoin in 2009, the world witnessed the birth of a decentralized digital currency that operates on a Peer-to-Peer (P2P) network, bypassing the need for intermediaries such as banks or governments. Since then, thousands of cryptocurrencies have emerged, each with its own unique features and use cases, further fueling the evolution of decentralized finance.

At the core of these digital currencies lies the concept of a P2P network, which forms the backbone of transactions and consensus mechanisms. P2P networks enable direct communication and interaction between participants, allowing for trust less transactions and ensuring the integrity of the system through distributed consensus mechanisms like Proof of Work (POW) or Proof of Stake (POS). Understanding the dynamics of these networks is crucial for assessing their efficiency, scalability, and security.

Our project aims to delve deep into the workings of P2P cryptocurrency networks by developing a sophisticated discrete-event simulator. Through this simulator, we seek to model various aspects of network behavior, including transaction generation, network topology, latency simulation, mining algorithms, block propagation, and blockchain maintenance. By simulating these components, we aim to gain insights into the performance and resilience of P2P networks under different conditions, paving the way for further research and optimization in decentralized systems.

2 Background

Cryptocurrencies have emerged as a disruptive force in the financial landscape, offering decentralized and transparent systems for peer-to-peer transactions. At the heart of these digital currencies lies their underlying network architecture, facilitating secure and efficient exchange among participants.

The motivation behind our project stems from the need to comprehensively understand the dynamics of peer-to-peer cryptocurrency networks. By developing a discrete-event simulator, we aim to delve into the intricacies of these networks, exploring their scalability, security, and performance under varying conditions.

Our objectives center on constructing a simulator that accurately models key components of a peer-to-peer cryptocurrency network. This includes transaction generation, network topology emulation, latency simulation, transaction forwarding mechanisms, and the implementation of proof-of-work consensus.

While our simulator may not capture every nuance of real-world cryptocurrency networks, it provides a valuable tool for studying their behavior. By focusing on essential functionalities and employing discrete-event simulation techniques, we aim to offer insights into network dynamics and potential areas for optimization.

In summary, our project seeks to provide a concise yet comprehensive simulation platform for analyzing peer-to-peer cryptocurrency networks. Through this endeavor, we hope to contribute to the ongoing discourse surrounding the future of decentralized financial systems.

3 Theoretical proofs

Theoretical reasons for choosing the exponential distribution for transaction inter-arrival time.

We can proof it theoretically and mathematically that the transaction inter arrival time follows the exponential distribution. Let consider a time interval of size Δ. As transactions are uniformly likely to occur at any point in time, the probability that a transaction occurs within this interval is proportional to Δ. Let this probability be $\beta\Delta$.

Then, assuming $t = 0$ marks a transaction, the probability that the next transaction occurs after n such time intervals is given by:

$$\Pr[t > n\Delta] = (1 - \beta\Delta)^n,$$

since it is equal to the probability that there is no transaction in each of n intervals of size Δ. Rewriting this with $T = n\Delta$, we have:

$$\lim_{n\to\infty} \left(1 - \frac{\beta T}{n}\right)^n = e^{-\beta T},$$

and thus $\Pr[t > T] = e^{-\beta T}$, which implies $\Pr[t \leq T] = 1 - e^{-\beta T}$.

To generalize the above probability to arbitrary and continuous values of T, suppose the intervals of size Δ are infinitesimally small, i.e., $\Delta \to 0$, and consequently $n = \frac{T}{\Delta}$.

Taking the limit as $n \to \infty$, we have:

$$\lim_{n\to\infty} \left(1 - \frac{\beta T}{n}\right)^n = e^{-\beta T},$$

and thus $\Pr[t > T] = e^{-\beta T}$, which implies $\Pr[t \leq T] = 1 - e^{-\beta T}$.

The latter is exactly the cumulative distribution function (CDF) of an exponential distribution having mean $\frac{1}{\beta}$. Thus, we sample transaction inter-arrival time from an exponential distribution having mean $T_{\text{tx}} = \frac{1}{\beta}$, for which the probability distribution function (PDF) is:

$$p(t = T) = \frac{1}{T_{\text{tx}}} e^{-\frac{T}{T_{\text{tx}}}}.$$

Therefore, we choose transaction inter-arrival time to be sampled from an exponential distribution

Why is the mean of d_{ij} inversely related to c_{ij} ?

The inverse relationship between the mean queueing delay d_{ij} and the link speed c_{ij} can be attributed to fundamental principles of queuing theory in network communication. In essence, the queueing delay at node i to forward a message to node j is contingent upon the speed of the link connecting these nodes, denoted by c_{ij}.

The queueing delay experienced by a packet in a queue is directly influenced by the number of packets queued before it. In a scenario where the link speed towards the destination is high, a greater number of packets can be processed and removed from the queue per unit time. Consequently, the waiting time for a specific packet, such as packet P, to be dequeued is diminished.

Formally, if each packet in the queue has a size of k bits and the link speed is c bits per second, the queueing delay for packet P can be expressed as:

$$d = \frac{\text{number of bits queued before } P}{Speed} = \frac{\text{number of bits queued before } P}{\text{link speed } c}$$

This formulation highlights the inverse proportionality between the mean queueing delay d_{ij} and the link speed c_{ij}. As the link speed increases, the queueing delay diminishes proportionally, aligning with the intuitive expectation that higher link speeds facilitate swifter packet processing and transmission.

4 Visualization and Analysis

There are n peers, each with a unique ID, where n is set at the time of initiation of the network. Some of these nodes (say z0 percent, where z_0 is a command line simulation parameter) are labeled "slow" and the others "fast". In addition, some of these nodes (say z_1 percent, where z1 is a command line simulation parameter) are labeled "low CPU" and the others "high CPU".

4.1 Analysis of first Simulation

This simulation incorporates the standard values of T_{tx} and T_k. Notably, T_k exceeds T_{tx} significantly. We've chosen to maintain T_{tx} at 1 seconds, reflecting the average transaction inter arrival time across networks discussed in lectures. Meanwhile, T_k is set at 200 seconds representing a prevalent scenario.

4.1.1 Experiment Parameters:

SAVE RESULTS : True
NUMBER OF PEERS : 20
Z0 : 0.7
Z1 : 0.8
AVG TXN INTERVAL TIME (Ttx) : 10000
AVG BLOCK MINING TIME (Tk) : 1000000
TARGET NUMBER OF BLOCKS : 300
NUMBER OF TXNS PER BLOCK : 100
NUMBER OF TRANSACTIONS : 30000
NUMBER OF TRANSACTIONS PER PEER : 1500.0
BLOCK TXNS MAX THRESHOLD : 1000
BLOCK TXNS MIN THRESHOLD : 50
BLOCK TXNS TRIGGER THRESHOLD : 100
INITIAL COINS : 1000
EVENT QUEUE TIMEOUT : 5

4.1.2 Results:

Total blocks: 273
Longest chain: 273
Longest chain/Total blocks: 1.0

hashing power	network speed	average longest chain contribution
low	low	2.5
low	high	1.56
high	low	20.02
high	high	-

Table 1: Average ration for peer types

4.1.3 Statistics

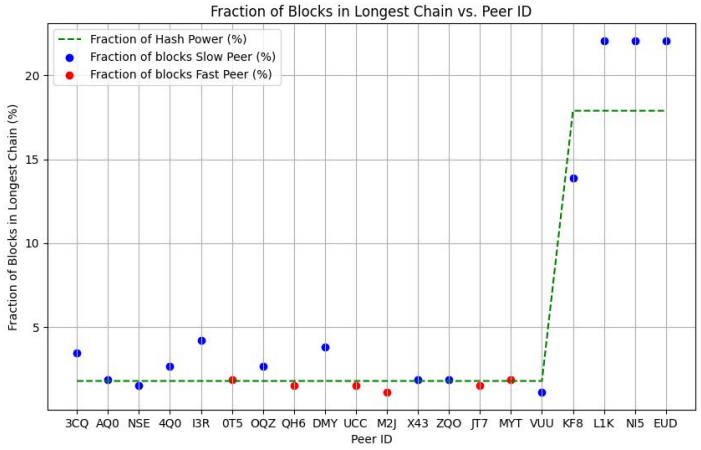

Figure 1: Contribution ration vs Peer power

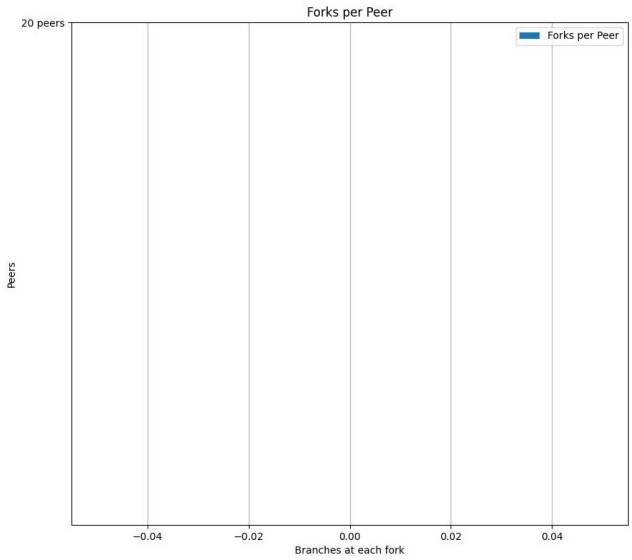

Figure 2: Fork statistics of first Simulation

The high ratio of the longest chain length to the total number of blocks can be attributed to the elevated value of T_k. With T_k set at approximately one second, significantly surpassing the time taken by a mined block to propagate across the entire network, occurrences of forks are notably absent. This observation is further emphasized in the blockchain tree plot depicted below.

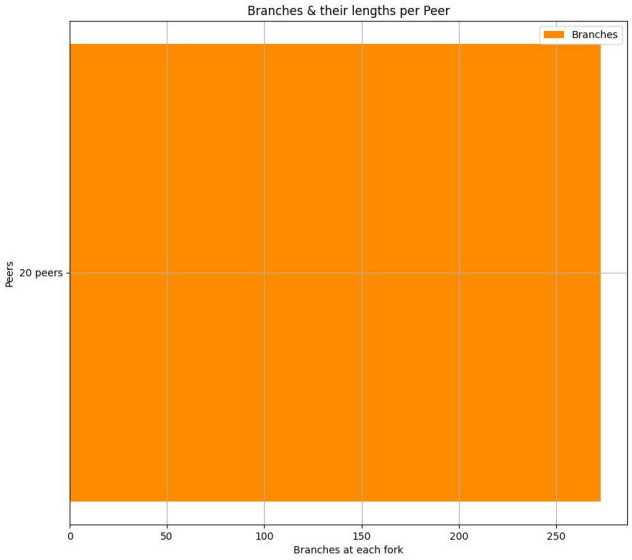

Figure 3: Branch statistics of first Simulation

4.1.4 Blockchain Tree

To analyze the behavior of each peer, we chart the proportion of blocks it contributes to the longest chain against the total number of blocks in that chain. Ideally, this ratio should primarily reflect the peer's mining power, with network propagation effects being less influential in typical scenarios. This assertion is corroborated by our visual representation, indicating that network latency, as exemplified by the Slow and Fast peers, plays a comparatively minor role in determining the ratio of blocks within the longest chain compared to hashing power.

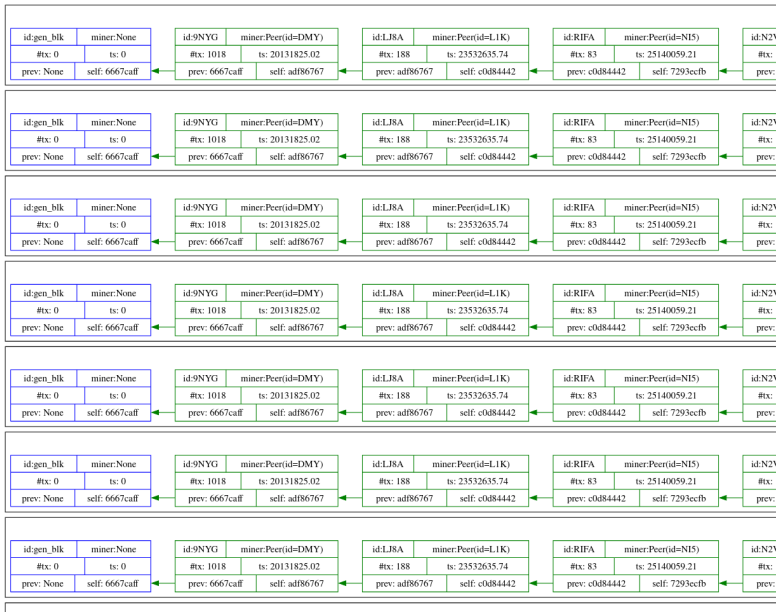

Figure 4: Blockchain for first simulation

4.2 Analysis of Second Simulation

In this scenario, we equalize T_k to T_{tx} and set the total number of generated blocks to 100, which are the only modifications from the initial simulation. With the reduction in the average mining time (T_k), we anticipate an increased occurrence of forks. This is due to the higher likelihood of new blocks being mined before a previously mined block is disseminated to all nodes.

4.2.1 Experiment Parameters:

SAVE RESULTS : True
NUMBER OF PEERS : 20
Z0 : 0.7
Z1 : 0.8
AVG TXN INTERVAL TIME : 10000
AVG BLOCK MINING TIME : 10000
TARGET NUMBER OF BLOCKS : 300
NUMBER OF TXNS PER BLOCK : 100
NUMBER OF TRANSACTIONS : 30000
NUMBER OF TRANSACTIONS PER PEER : 1500.0
BLOCK TXNS MAX THRESHOLD : 1000
BLOCK TXNS MIN THRESHOLD : 50
BLOCK TXNS TRIGGER THRESHOLD : 100
INITIAL COINS : 1000
EVENT QUEUE TIMEOUT : 5

4.2.2 Results:

Total blocks: 306
Longest chain: 292
Longest chain/Total blocks: 0.95

hashing power	network speed	average longest chain contribution
low	low	2.08
low	high	2.1
high	low	21.91
high	high	18.64

Table 2: Average ration for peer types

4.2.3 Statistics

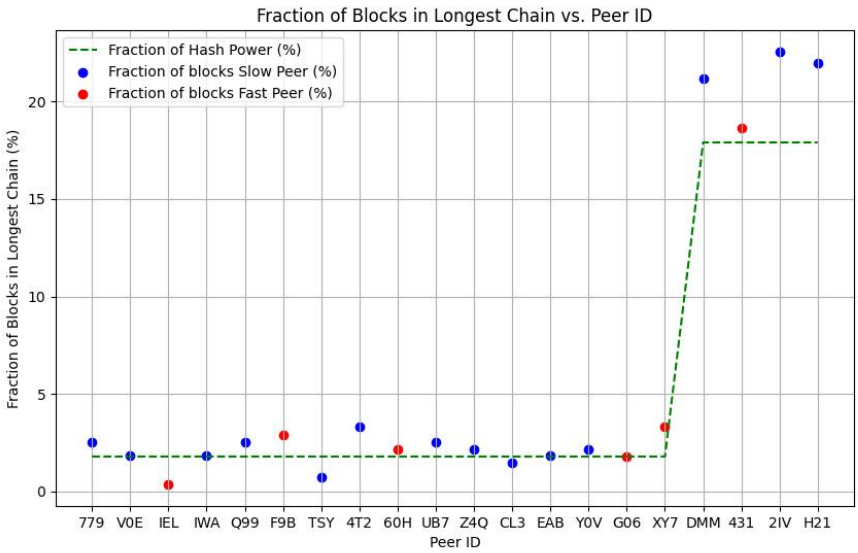

Figure 5: Contribution ration vs Peer power

The obtained results confirm our expectation of a significant increase in fork occurrences and subsequent rejection of a greater number of blocks. Consequently, the ratio of the longest chain's length to the total number of blocks in the blockchain declines to 0.95 from 1.0 in the initial simulation. Additionally, we observe diminished fractions of blocks incorporated into the longest chain across all four categories. This reduction stems from the increased frequency of forks, resulting in a greater number of blocks failing to join the longest chain and consequently yielding lower fractions.

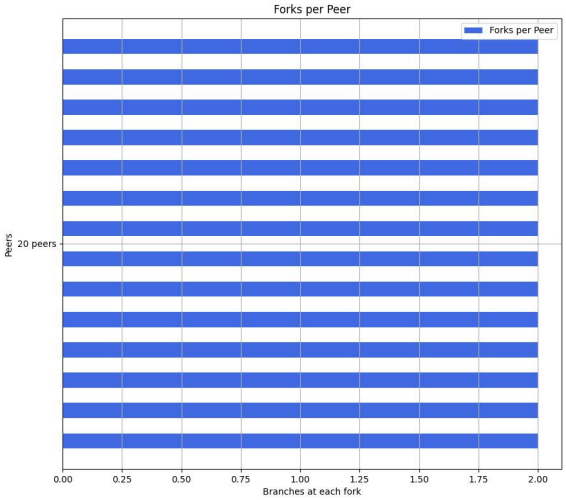

Figure 6: Fork statistics of second Simulation

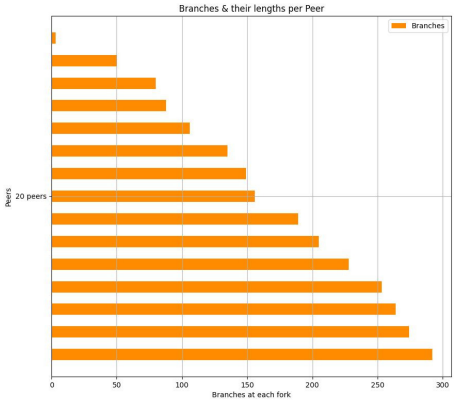

Figure 7: Branch statistics of second Simulation

4.2.4 Blockchain Tree

Examining peer-level statistics, we observe a greater variability in the proportion of blocks within the longest chain, with its dependency on hashing power diminished. This shift can be attributed to the reduced T_k, resulting in a less pronounced impact of variations in hashing power. Peer Statistics.

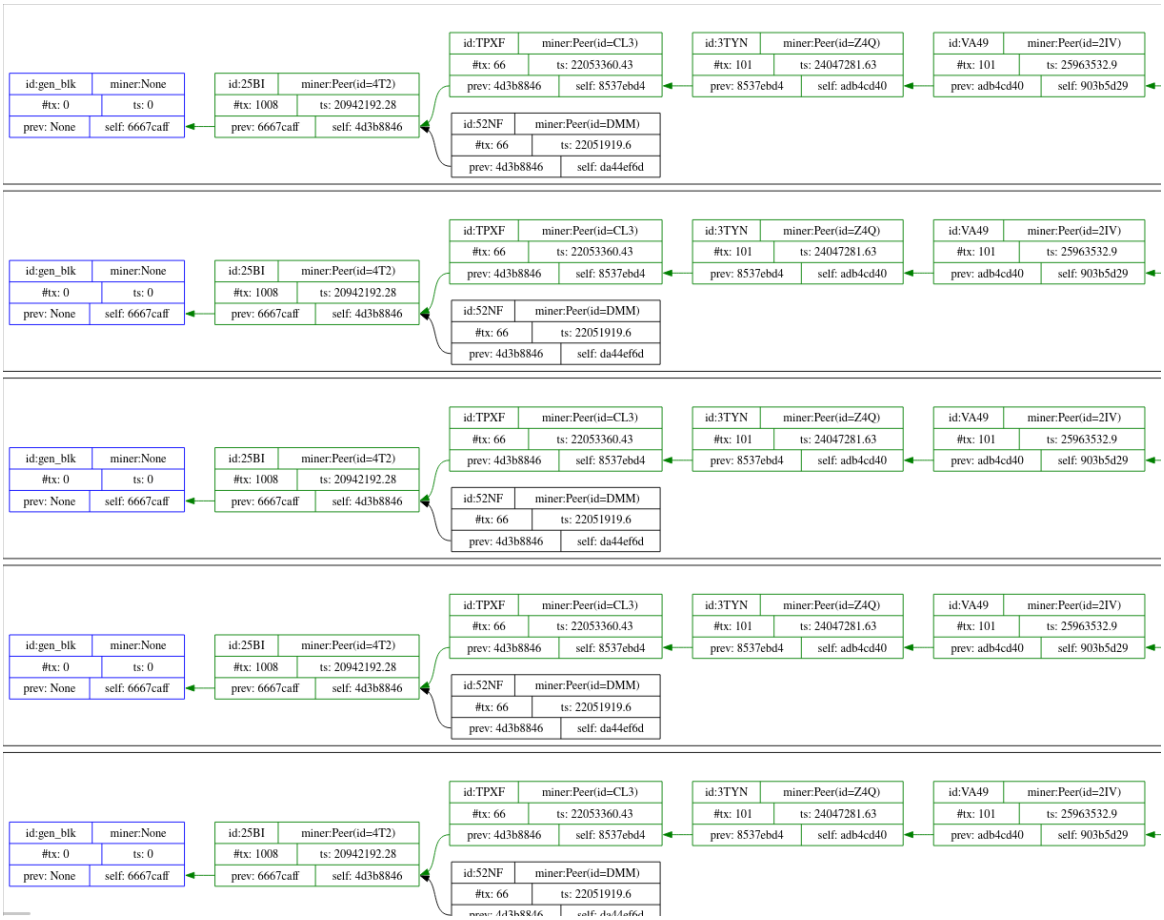

Figure 8: Blockchain for second simulation

4.3 Analysis of Third Simulation

In this simulation, we further decrease both T_{tx} and T_k. Notably, this experiment holds significance as both T_{tx} and T_k are now lower than the network's link speeds.

With the mining and transaction creation rates surpassing the network's link speeds, an influx of blocks floods the network, leading to an escalation in fork occurrences. Consequently, the ratio of the longest chain to the total number of blocks decreases even further.

4.3.1 Experiment Parameters:

SAVE RESULTS : True
NUMBER OF PEERS : 20
Z0 : 0.7
Z1 : 0.8
AVG TXN INTERVAL TIME : 10000
AVG BLOCK MINING TIME : 1000
TARGET NUMBER OF BLOCKS : 300
NUMBER OF TXNS PER BLOCK : 100
NUMBER OF TRANSACTIONS : 30000
NUMBER OF TRANSACTIONS PER PEER : 1500.0
BLOCK TXNS MAX THRESHOLD : 1000
BLOCK TXNS MIN THRESHOLD : 50
BLOCK TXNS TRIGGER THRESHOLD : 100
INITIAL COINS : 1000
EVENT QUEUE TIMEOUT : 5

4.3.2 Results:

Total blocks: 306
Longest chain: 230
Longest chain/Total blocks: 0.75

hashing power	**network speed**	**average longest chain contribution**
low	low	1.91
low	high	2.59
high	low	20.19
high	high	-

Table 3: Average ration for peer types

4.3.3 Statistics

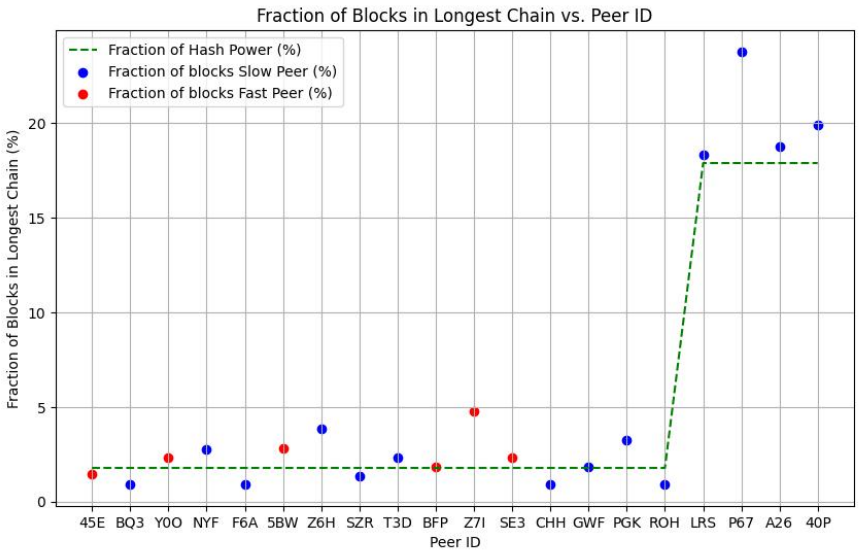

Figure 9: Contribution ration vs Peer power

Since the mining and transaction creation rate is higher than the network link speeds, we get an increased amount of forking as the network is now flooded with blocks. Thus the longest chain to total blocks ratio further reduces.

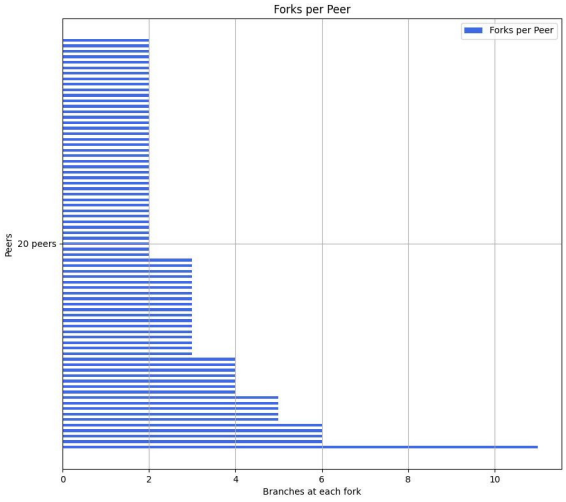

Figure 10: Fork statistics of third Simulation

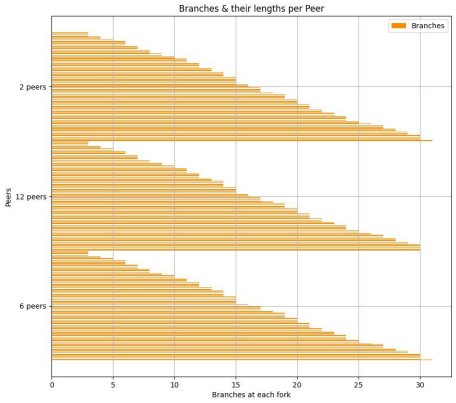

Figure 11: Branch statistics of third Simulation

4.3.4 Blockchain Tree

At the peer level, a minimal number of blocks make it into the longest chain, and a considerable portion of the blocks face rejection. Consequently, only a limited number of users have their blocks present in the network, while the majority of other nodes have zero blocks in the network.

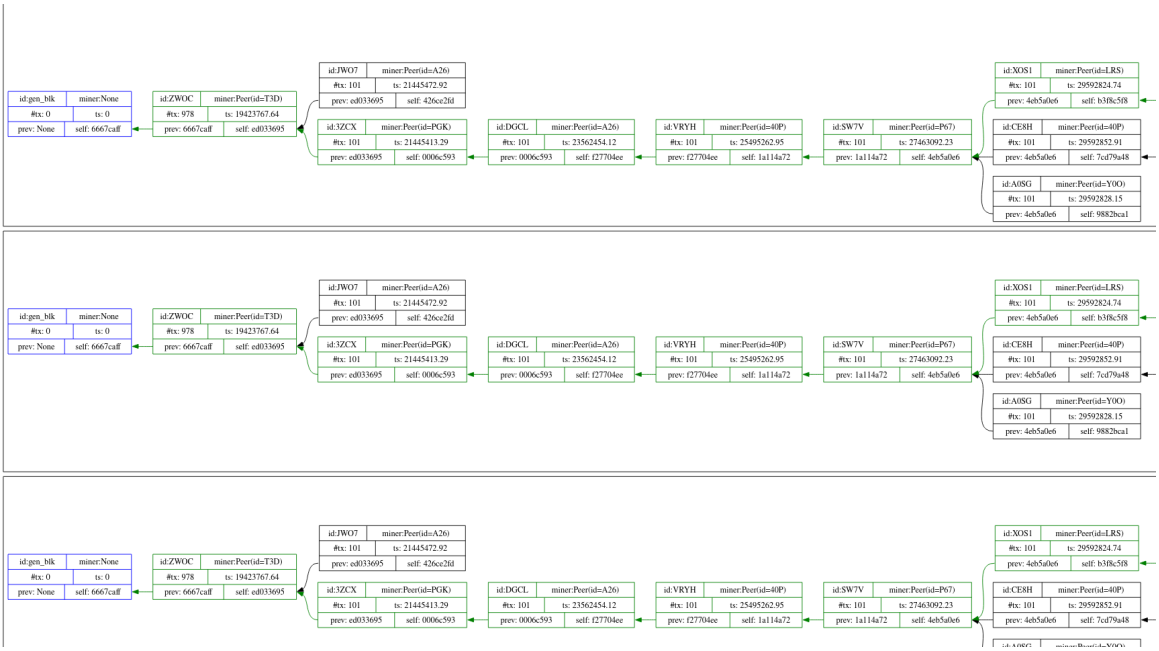

Figure 12: Blockchain for third simulation

4.4 Analysis of fourth Simulation

In this simulation, we decrease transaction interval time and block generation time less than network delay.

4.4.1 Experiment Parameters:

SAVE RESULTS : True
NUMBER OF PEERS : 20
Z0 : 0.7
Z1 : 0.8
AVG TXN INTERVAL TIME : 10
AVG BLOCK MINING TIME : 10
TARGET NUMBER OF BLOCKS : 300
NUMBER OF TXNS PER BLOCK : 100
NUMBER OF TRANSACTIONS : 30000
NUMBER OF TRANSACTIONS PER PEER : 1500.0
BLOCK TXNS MAX THRESHOLD : 1000
BLOCK TXNS MIN THRESHOLD : 50
BLOCK TXNS TRIGGER THRESHOLD : 100
INITIAL COINS : 1000
EVENT QUEUE TIMEOUT : 5

4.4.2 Results:

Total blocks: 301
Longest chain: 31
Longest chain/Total blocks: 0.1

hashing power	**network speed**	**average longest chain contribution**
low	low	3.63
low	high	4.34
high	low	9.32
high	high	21.43

Table 4: Average ration for peer types

4.4.3 Statistics

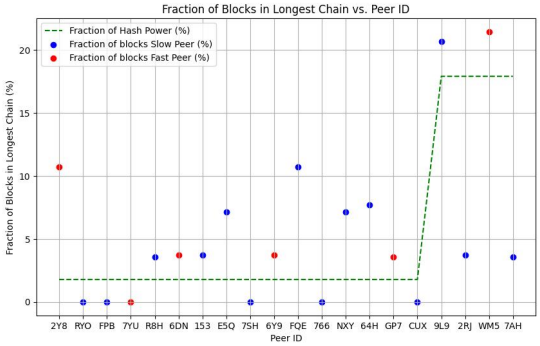

Figure 13: Contribution ration vs Peer power

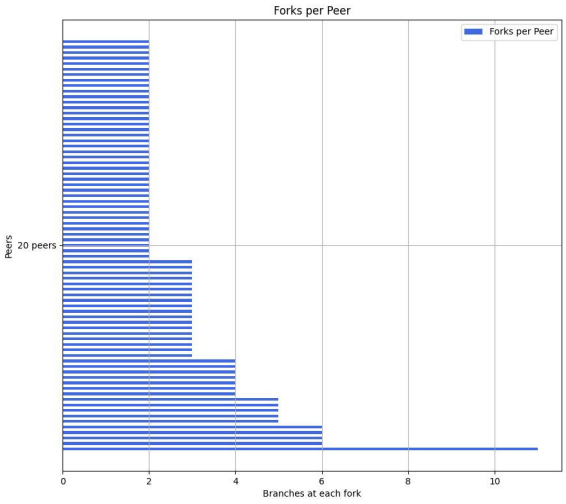

Figure 14: Fork statistics of fourth Simulation

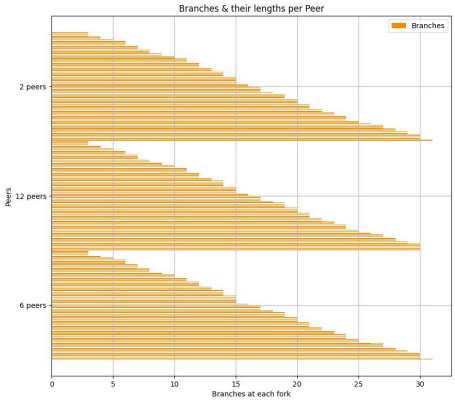

Figure 15: Branch statistics of fourth Simulation

4.4.4 Blockchain Tree

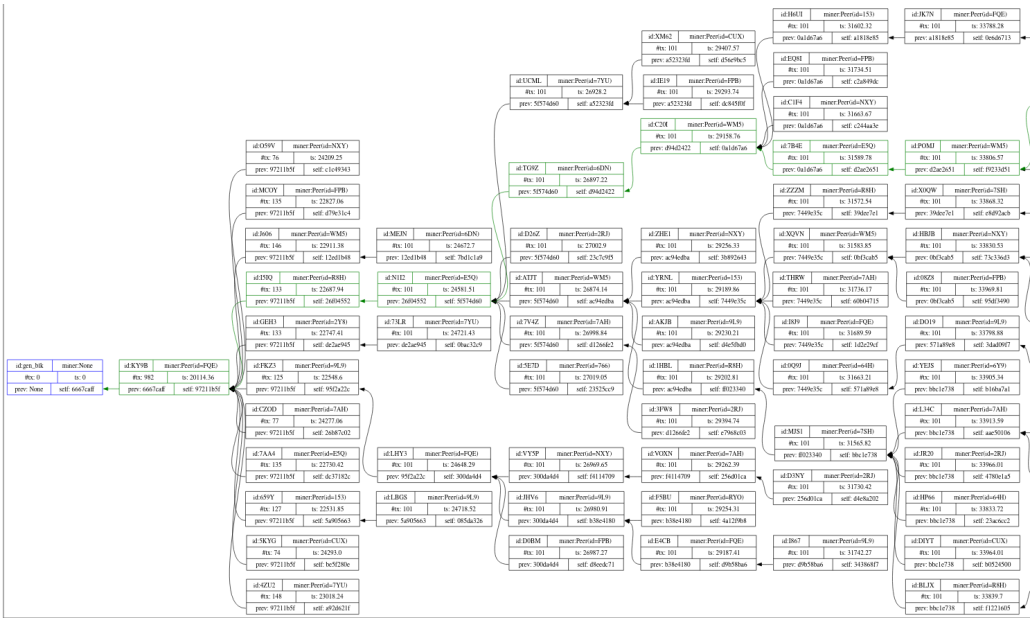

Figure 16: Blockchain for fourth simulation

5 References

1. Title of Lecture 10. [Online] Available: https://people.orie.cornell.edu/mru8/orie3120/lec/lec10.pdf [Accessed on February 16, 2024].

2. Title of Chapter 3. [Online] Available: http://cs.baylor.edu/~maurer/aida/desauto/chapter3.pdf [Accessed on February 16, 2024].

3. Introduction to Discrete Event Systems. [Online] Available: https://www.cs.cmu.edu/~music/cmsip/readings/intro-discrete-even [Accessed on February 16, 2024].

4. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system", Decentralized Business Review, pp. 21260, 2008.

5. M. Jakobsson and A. Juels, "Proofs of work and bread pudding protocols", Secure information networks, pp. 258-272, 1999.