Introduction to Blockchains

Course Code - CS765

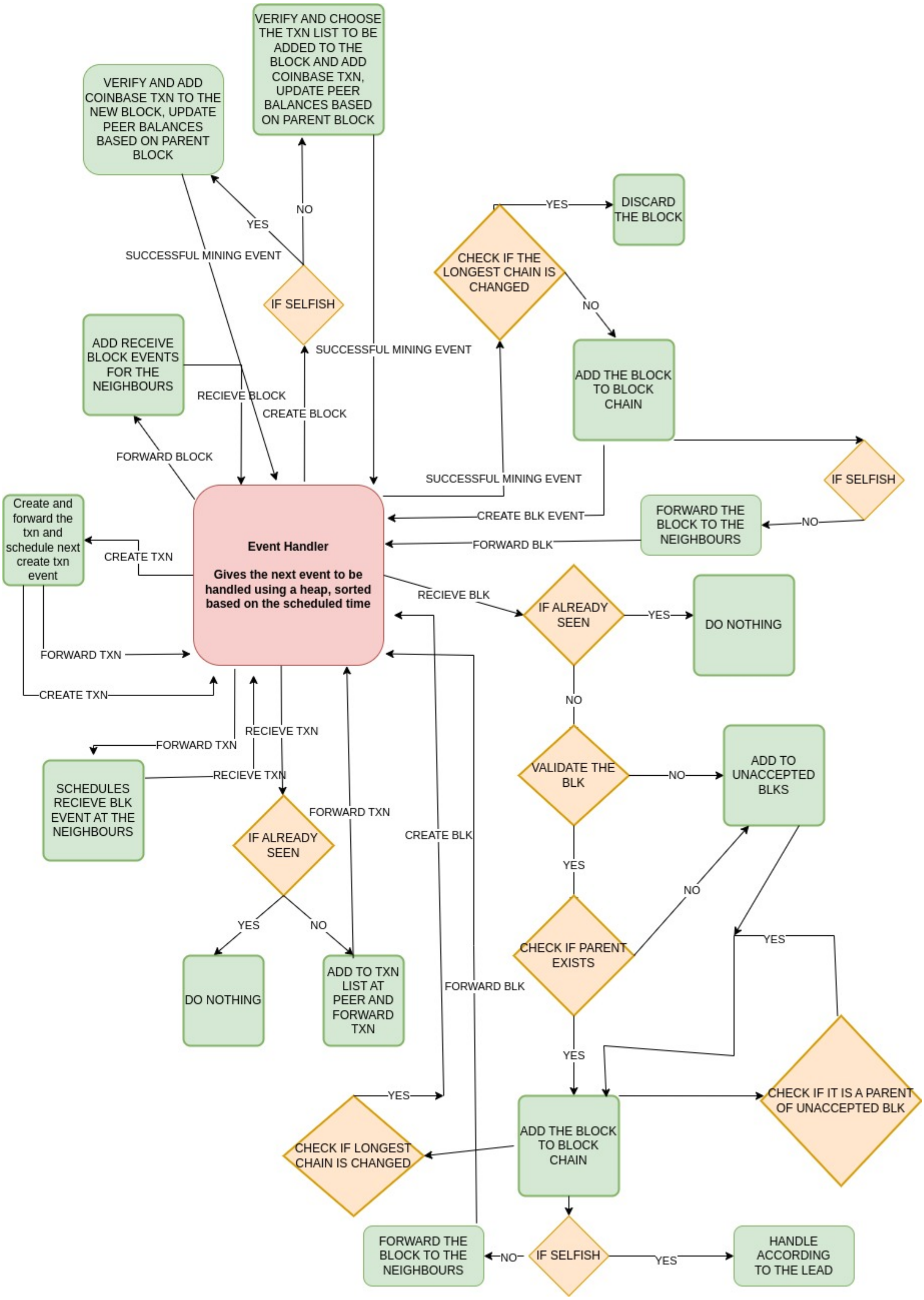
Assignment 2

Report

210050105,210050098,210050034

March 2024

1 Code Flow



VERIFY AND CHOOSE THE TXN LIST TO BE ADDED TO THE BLOCK AND ADD COINBASE TXN, UPDATE PEER BALANCES BASED ON PARENT BLOCK
VERIFY AND ADD COINBASE TXN TO THE NEW BLOCK, UPDATE PEER BALANCES BASED ON PARENT BLOCK
NO
YES
SUCCESSFUL MINING EVENT
IF SELFISH
YES
DISCARD THE BLOCK
CHECK IF THE LONGEST CHAIN IS CHANGED
NO
SUCCESSFUL MINING EVENT
ADD RECEIVE BLOCK EVENTS FOR THE NEIGHBOURS
RECIEVE BLOCK
CREATE BLOCK
ADD THE BLOCK TO BLOCK CHAIN
FORWARD BLOCK
SUCCESSFUL MINING EVENT
IF SELFISH
Create and forward the txn and schedule next create txn event
CREATE BLK EVENT
FORWARD THE BLOCK TO THE NEIGHBOURS
NO
Event Handler
Gives the next event to be handled using a heap, sorted based on the scheduled time
FORWARD BLK
CREATE TXN
RECIEVE BLK
IF ALREADY SEEN
YES
DO NOTHING
FORWARD TXN
CREATE TXN
NO
RECIEVE TXN
FORWARD TXN
VALIDATE THE BLK
NO
ADD TO UNACCEPTED BLKS
SCHEDULES RECIEVE BLK EVENT AT THE NEIGHBOURS
RECIEVE TXN
FORWARD TXN
IF ALREADY SEEN
CREATE BLK
YES
YES
NO
NO
DO NOTHING
ADD TO TXN LIST AT PEER AND FORWARD TXN
FORWARD BLK
CHECK IF PARENT EXISTS
YES
YES
YES
CHECK IF IT IS A PARENT OF UNACCEPTED BLK
CHECK IF LONGEST CHAIN IS CHANGED
ADD THE BLOCK TO BLOCK CHAIN
FORWARD THE BLOCK TO THE NEIGHBOURS
NO
IF SELFISH
YES
HANDLE ACCORDING TO THE LEAD

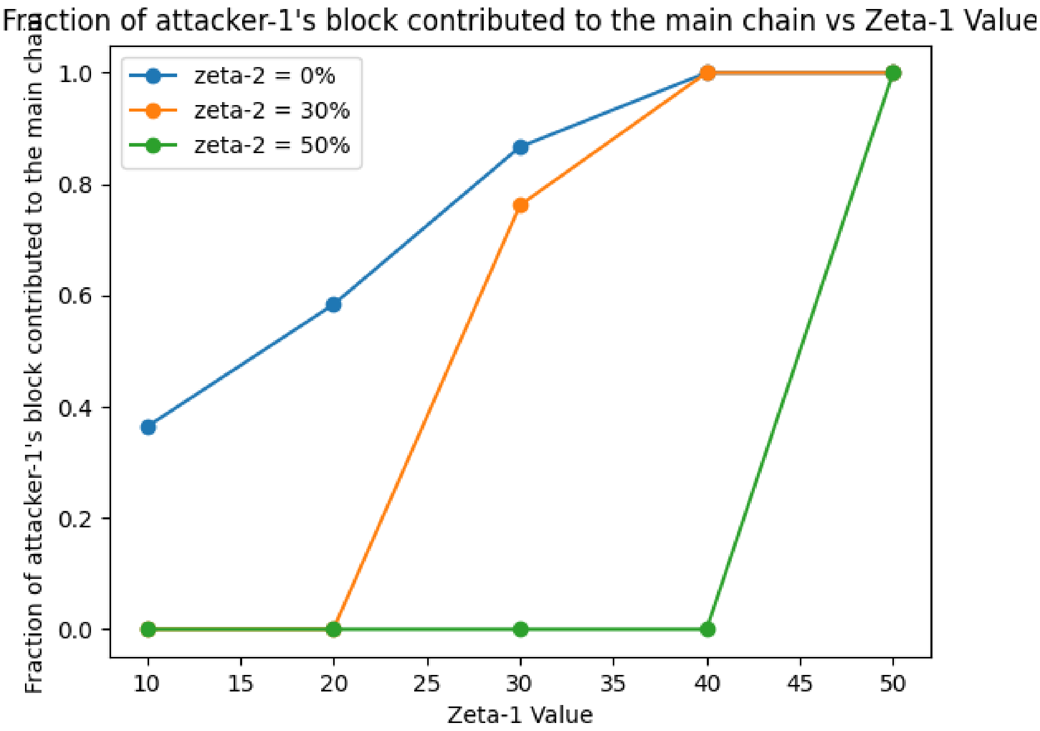
2 Assumptions

- The blocks with the red border indicate the blocks created by adversary 1
- The blocks with the blue border indicate the blocks created by adversary 2
- The block with a green border indicates the last block of the longest chain of that Node
- All the analysis is made by keeping 20 peers, and transaction inter-arrival time as 10ms and block inter-arrival time as 100ms So that latency also comes into effect
- At the end of the Simulation all the blocks stored by the selfish nodes are released, so the effect of selfish mining can be shown.

3 Paramters

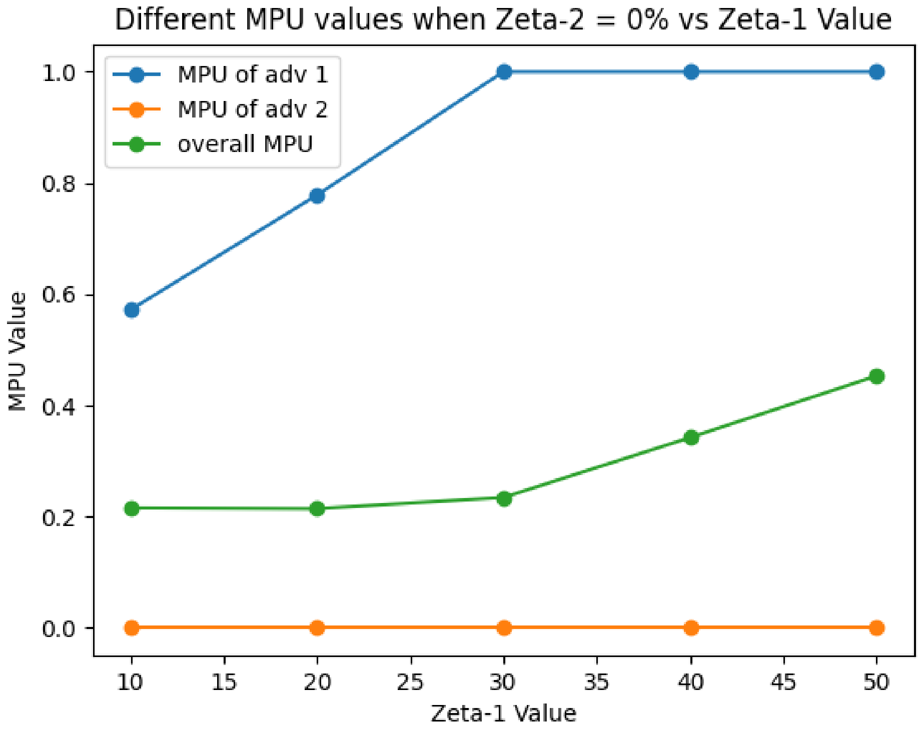
Fraction of attacker's block = $\frac{\text{No of blocks of attacker in the longest chain}}{\text{Total no of blocks in the longest chain}}$

4 Graphs and Analysis



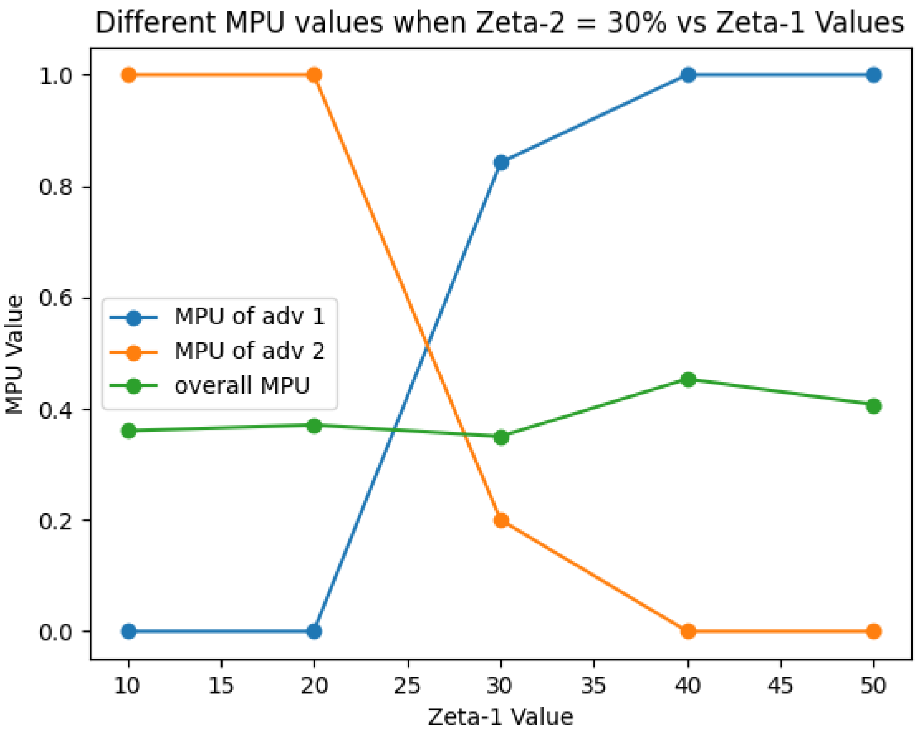
- Consider the case when zeta-2 = 0 (i.e. second adversary does not contribute anything), as the hashing power increases the fraction of the blocks contributed by the attacker increases because the attacker can produce more blocks due to increased hashing power.
- When the zeta-2 = 30% , if the zeta-1 is less than zeta-2 the attacker-1 often loses his secret chain to the attacker-2, as attacker-1 can produce at faster rate
- If zeta-1 is more than zeta-2, the attacker-1 will have a sudden increase in the fraction value, because the attacker-1 produces at a faster rate

- When the zeta-2 is around 50%, it leads 51% attack and attacker-2 can outrun any longer chain, when both become 50%, one of them will have fraction = 1

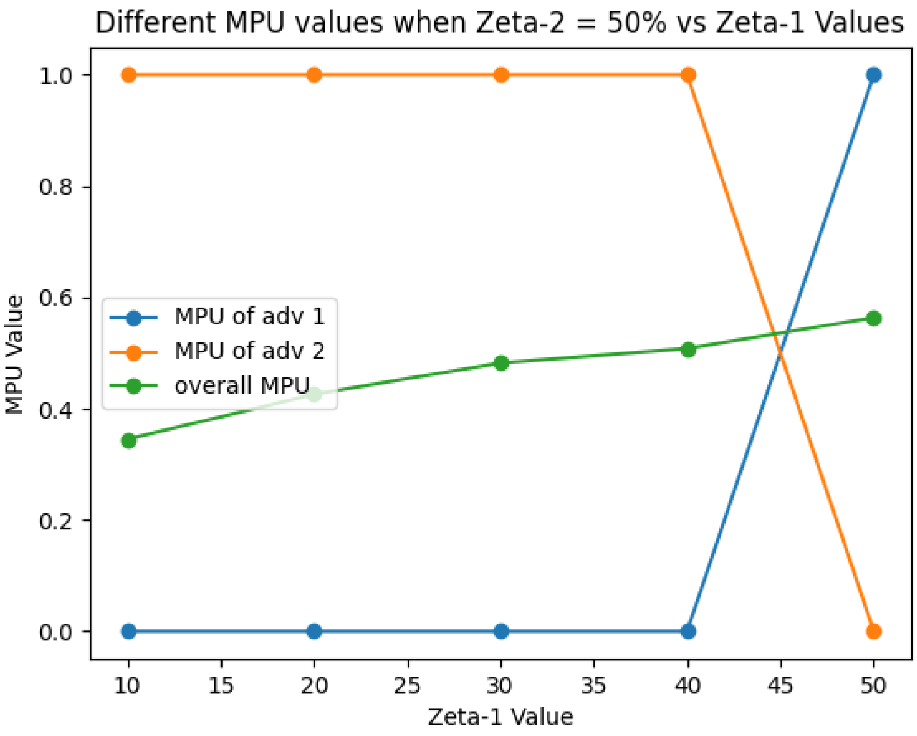


Note: MPU is the fraction of blocks in the main chain by no of blocks created

- Since attacker-2 has 0 hashing power, he cannot produce any blocks, so his MPU value will be 0
- when zeta-1 = 10%, it does not have enough power to override the network, so around half of its blocks are not in the main chain
- When the zeta-1 becomes around 35-40% if there is a fork, it has enough hashing power to override the network
- As the hashing power increases, the overall MPU value approaches 0.5, because the attacker-1 maintains a secret chain, and releases the block only when an honest block is released, this leads to two sets of blocks with almost equal no of blocks in them.

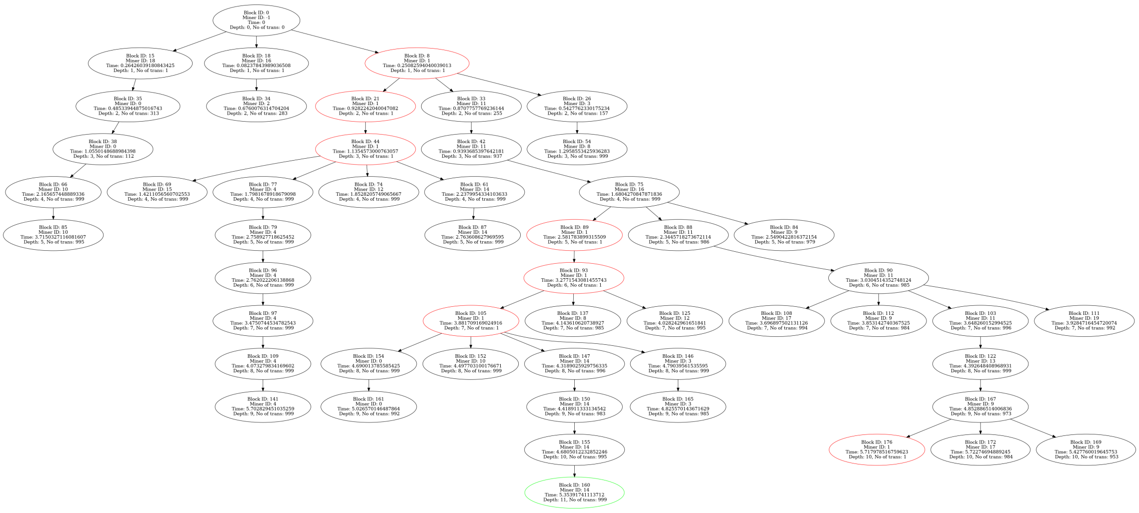


- Here zeta-2 is 30% so, attacker-2 can override the network and make sure his blocks can get into the main chain, if attacker-1 has less power than attacker-2, he cannot override the network.
- Similarly if zeta-1 is greater than then the attacker-2 cannot overtake attacker-1, so MPU almost reaches 1 for attacker 1 and 0 for attacker 2, as honest miners only have around 30% of the power

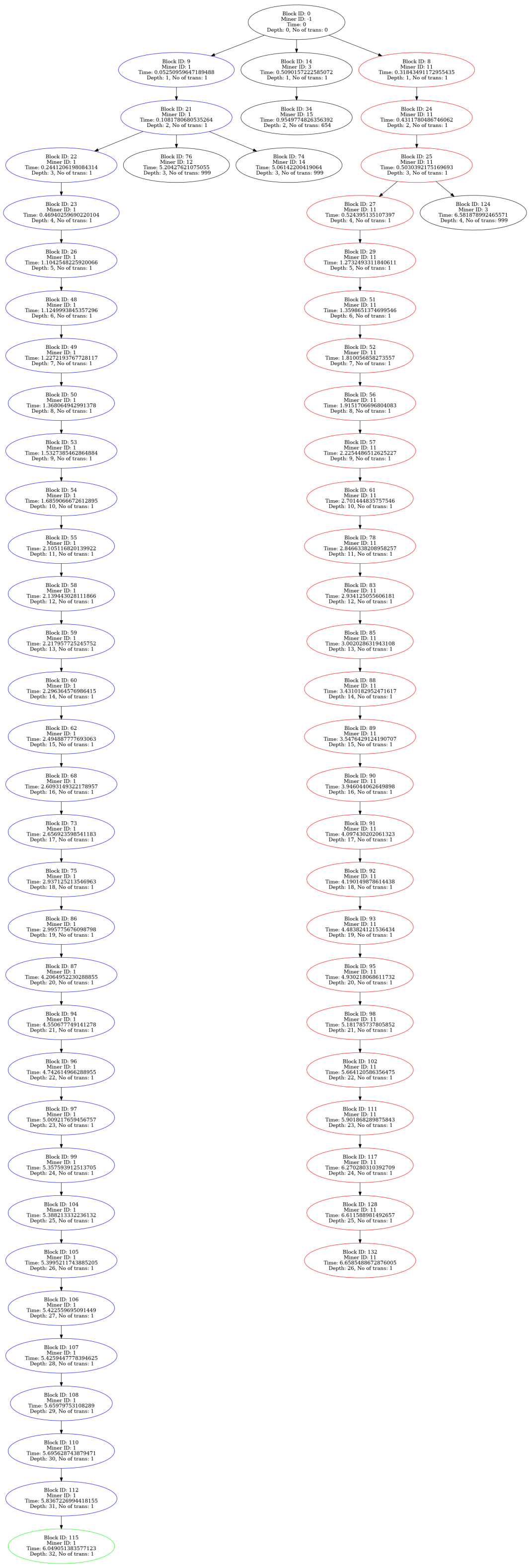


- Here zeta-2 = 50%, so the attacker-1 will have MPU 1, and attacker-2 will have 0 because he cannot overtake attacker-2
- Similar to the above case, attacker-2 maintains a secret chain, and releases the block only when an honest block is released, this leads to two sets of blocks with almost equal no of blocks in them

5 Some More observations



This is the block diagram when the no of peers = 20, and zeta1 = 10, zeta2=0



This is the block diagram when the no of peers = 20, and zeta1 = 40, zeta2=50

There is more branching when all the nodes have almost equal hashing power and less branching when 2 attackers have almost all the hashing power.