Report on: Simulating a selfish mining attack using the P2P Cryptocurrency Network

Assignment - 2

Akash Kumar (213050020)

Hrishikesh Saloi (213050057)

Manoj Kumar Maurya(213050067)

Contents

1 Introduction **3**

2 Observation of Blockchain trees by taking different values of parameters **4**

2.1 In Stubborn Mining attack 5

2.1.1 When n=10, $T_x = 40$, $T_{tx} = 10$, H = 0.25 5

2.1.2 When n=10, $T_x = 40$, $T_{tx} = 10$, H = 0.50 5

2.1.3 When n=10, $T_x = 40$, $T_{tx} = 10$, H = 0.75 5

2.1.4 When n=10, $T_x = 30$, $T_{tx} = 10$, H = 0.50 5

2.1.5 When n=10, $T_x = 60$, $T_{tx} = 10$, H = 0.50 5

2.1.6 When n=10, $T_x = 40$, $T_{tx} = 20$, H = 0.50 6

2.1.7 When n=10, $T_x = 40$, $T_{tx} = 60$, H = 0.50 6

2.1.8 When n=15, $T_x = 40$, $T_{tx} = 60$, H = 0.50 6

2.2 In Selfish Mining attack 7

2.2.1 When n=10, $T_x = 40$, $T_{tx} = 10$, H = 0.25 7

2.2.2 When n=10, $T_x = 40$, $T_{tx} = 10$, H = 0.50 7

2.2.3 When n=10, $T_x = 40$, $T_{tx} = 10$, H = 0.75 7

2.2.4 When n=10, $T_x = 30$, $T_{tx} = 10$, H = 0.50 7

2.2.5 When n=10, $T_x = 60$, $T_{tx} = 10$, H = 0.50 7

2.2.6 When n=10, $T_x = 40$, $T_{tx} = 20$, H = 0.50 8

2.2.7 When n=10, $T_x = 40$, $T_{tx} = 60$, H = 0.50 8

2.2.8 When n=15, $T_x = 40$, $T_{tx} = 60$, H = 0.50 8

3 Conclusion of Observations **9**

4 The Above Observation is based on following interconnection between the peer nodes **10**

4.1 interconnection between the 10 peer nodes 10

4.1.1 interconnection between the 15 peer nodes 10

5 Picture of blockchain trees and longest chain *Selfish Mining* **11**

5.1 Hashing Power .25 11

5.1.1 Blockchain Tree 11
5.1.2 Longest Chain 11
5.2 Hashing Power .50 12
5.2.1 Blockchain Tree 12
5.2.2 Longest Chain 12
5.3 Hashing Power .75 13
5.3.1 Blockchain Tree 13
5.3.2 Longest Chain 13

6 Picture of blockchain trees and longest chain *Stubborn Mining* 14
6.1 Hashing Power .25 14
6.1.1 Blockchain Tree 14
6.1.2 Longest Chain 14
6.2 Hashing Power .50 15
6.2.1 Blockchain Tree 15
6.2.2 Longest Chain 15
6.3 Hashing Power .75 16
6.3.1 Blockchain Tree 16
6.3.2 Longest Chain 16

7 Bibliography 17

1 Introduction

- In previous assignment we build our own discrete-event simulator for a P2P cryptocurrency network.

- Each peer is connected to a random number of other peers, such that the resulting network is connected.A node forwards any transaction heard from one peer to another connected peer, provided it has not already sent the same transaction to that peer, or provided it did not hear (receive) the transaction from that peer.

- Simulating PoW(Proof Of Work): All nodes have the genesis block at the start of the simulation. Each block have a unique ID, Any peer, say peer k, maintains a tree of blocks as in bitcoin. When it receives a block from another peer, it validates all its transactions (no balance of any peer should go negative), and if the block is valid it adds the block to its tree.

- Each node maintains a tree of all blockchains heard since the start of the simulation. The node stores the time of arrival of every block in its tree.

- Now in continuation of previous assignment on top of that we have implemented Simulation of selfish mining and stubborn mining attacks.

2 Observation of Blockchain trees by taking different values of parameters

All simulation is done for 200 events,

n - number of nodes or peer in the connected P2P network

T_x - Block Interarrival time mean

T_{tx} - Transaction Intearrival time mean

H - Hashing power of adversary

$$MPUnode_{adv} = \frac{\text{Number of block mined by an adversary in main chain}}{\text{Total number of blocks mined by an adversary}}$$

$$MPUnode_{overall} = \frac{\text{Number of block in the main chain}}{\text{Total number of blocks generated across all the nodes}}$$

2.1 In Stubborn Mining attack

Observations:

2.1.1 When n=10, $T_x = 40$, $T_{tx} = 10$, H = 0.25

$MPUnode_{adv} = 0.025$

$MPUnode_{overall} = 0.355$

2.1.2 When n=10, $T_x = 40$, $T_{tx} = 10$, H = 0.50

$MPUnode_{adv} = 0.459$

$MPUnode_{overall} = 0.358$

2.1.3 When n=10, $T_x = 40$, $T_{tx} = 10$, H = 0.75

$MPUnode_{adv} = 0.569$

$MPUnode_{overall} = .357$

2.1.4 When n=10, $T_x = 30$, $T_{tx} = 10$, H = 0.50

$MPUnode_{adv} = .40$

$MPUnode_{overall} = .387$

2.1.5 When n=10, $T_x = 60$, $T_{tx} = 10$, H = 0.50

$MPUnode_{adv} = 0.545$

$MPUnode_{overall} = .391$

2.1.6 When n=10, $T_x = 40$, $T_{tx} = 20$, H = 0.50

$MPUnode_{adv} = .462$

$MPUnode_{overall} = .389$

2.1.7 When n=10, $T_x = 40$, $T_{tx} = 60$, H = 0.50

$MPUnode_{adv} = .441$

$MPUnode_{overall} = .376$

2.1.8 When n=15, $T_x = 40$, $T_{tx} = 60$, H = 0.50

$MPUnode_{adv} = .380$

$MPUnode_{overall} = .287$

2.2 In Selfish Mining attack

Observations:

2.2.1 When n=10, $T_x = 40$, $T_{tx} = 10$, H = 0.25

$MPUnode_{adv} = .06$

$MPUnode_{overall} = .369$

2.2.2 When n=10, $T_x = 40$, $T_{tx} = 10$, H = 0.50

$MPUnode_{adv} = .4$

$MPUnode_{overall} = .352$

2.2.3 When n=10, $T_x = 40$, $T_{tx} = 10$, H = 0.75

$MPUnode_{adv} = .66$

$MPUnode_{overall} = .43$

2.2.4 When n=10, $T_x = 30$, $T_{tx} = 10$, H = 0.50

$MPUnode_{adv} = .25$

$MPUnode_{overall} = .3731$

2.2.5 When n=10, $T_x = 60$, $T_{tx} = 10$, H = 0.50

$MPUnode_{adv} = .66$

$MPUnode_{overall} = .3681$

2.2.6 When n=10, $T_x = 40$, $T_{tx} = 20$, H = 0.50

$MPUnode_{adv} = .45$

$MPUnode_{overall} = .432$

2.2.7 When n=10, $T_x = 40$, $T_{tx} = 60$, H = 0.50

$MPUnode_{adv} = .40$

$MPUnode_{overall} = .432$

2.2.8 When n=15, $T_x = 40$, $T_{tx} = 60$, H = 0.50

$MPUnode_{adv} = .40$

$MPUnode_{overall} = .305$

3 Conclusion of Observations

On changing hashing power,

- As hashing power increases value of $MPUnode_{adv}$ increases on both selfish and stubborn mining.
- As hashing power increases value of $MPUnode_{overall}$ does not change with a particular pattern (remains same) on both selfish and stubborn mining.

On changing value of T_k,

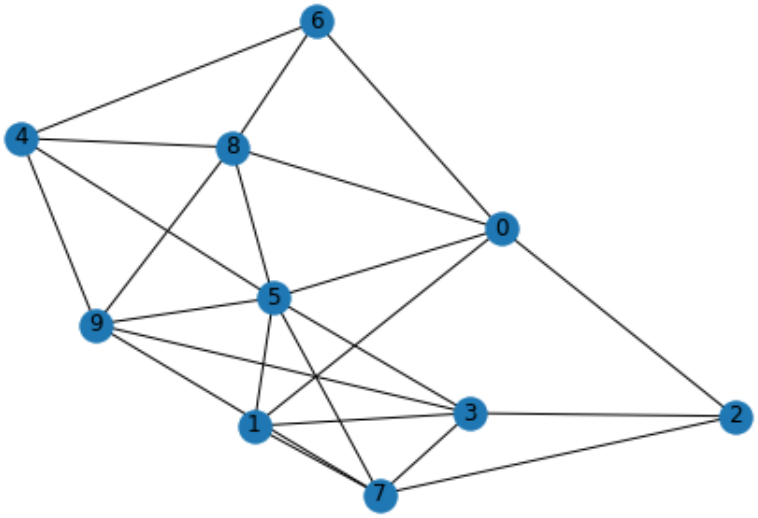
- As T_k increases value of $MPUnode_{adv}$ remains unchanged in both selfish and stubborn mining.
- As T_k increases value of $MPUnode_{overall}$ remains unchanged in both selfish and stubborn mining.

On changing value of T_{tx},

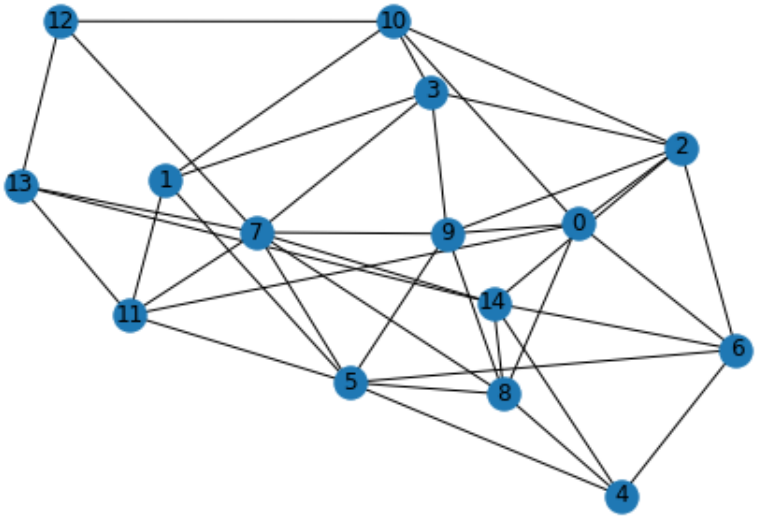
- As T_{tx} increases value of $MPUnode_{adv}$ remains unchanged in both selfish and stubborn mining.
- As T_{tx} increases value of $MPUnode_{overall}$ increases unchanged in both selfish and stubborn mining.

4 The Above Observation is based on following interconnection between the peer nodes

4.1 interconnection between the 10 peer nodes



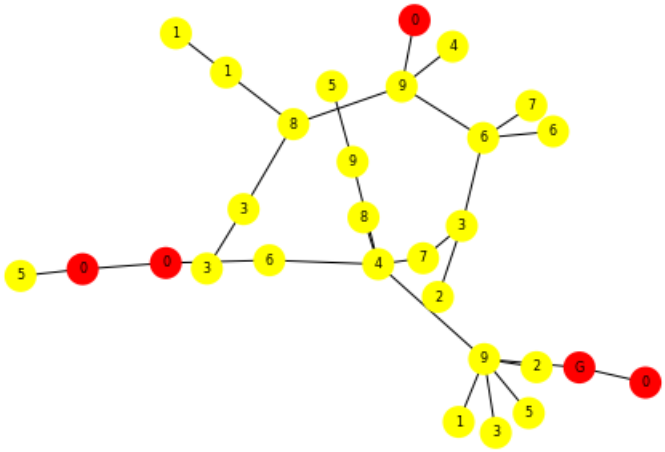
4.1.1 interconnection between the 15 peer nodes



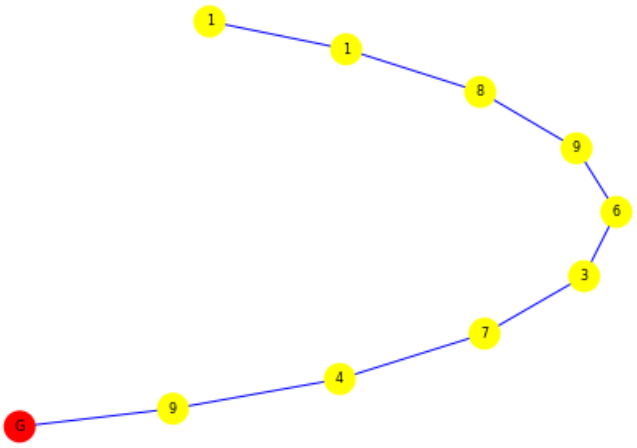
5 Picture of blockchain trees and longest chain *Selfish Mining*

5.1 Hashing Power .25

5.1.1 Blockchain Tree

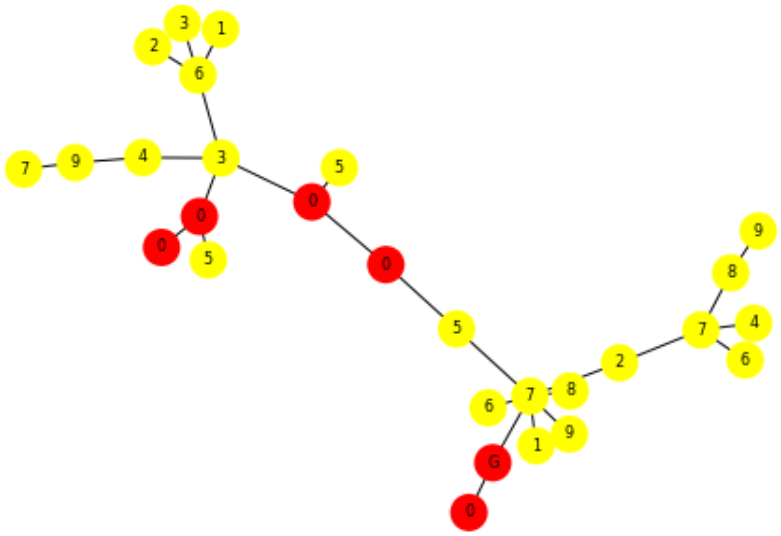


5.1.2 Longest Chain

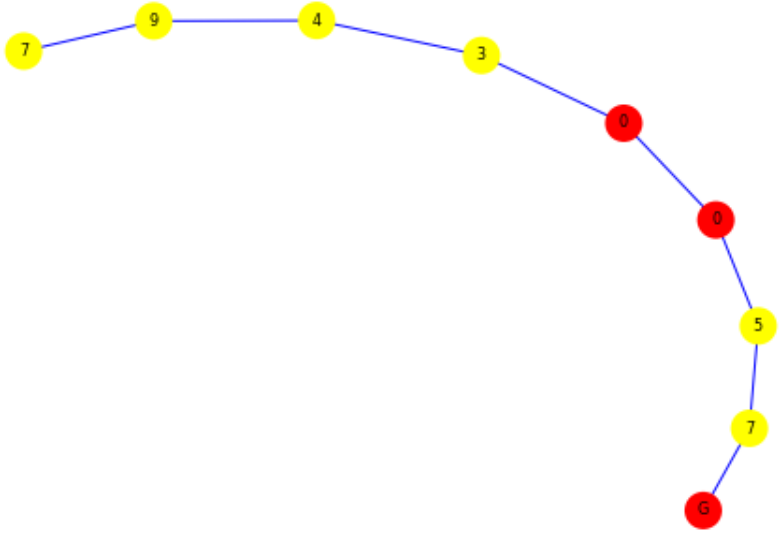


5.2 Hashing Power .50

5.2.1 Blockchain Tree

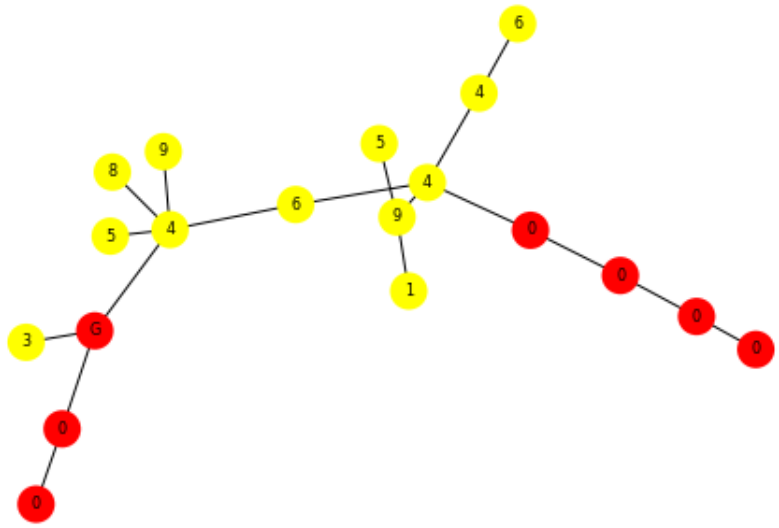


5.2.2 Longest Chain

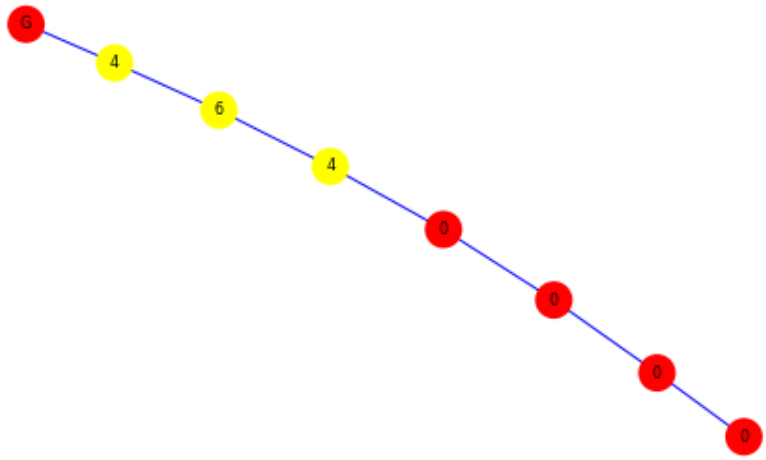


5.3 Hashing Power .75

5.3.1 Blockchain Tree



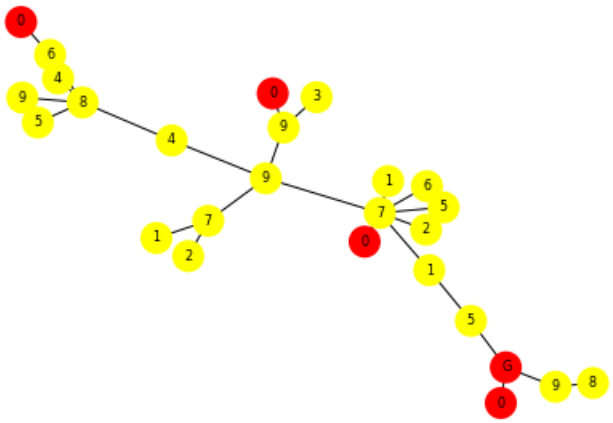
5.3.2 Longest Chain



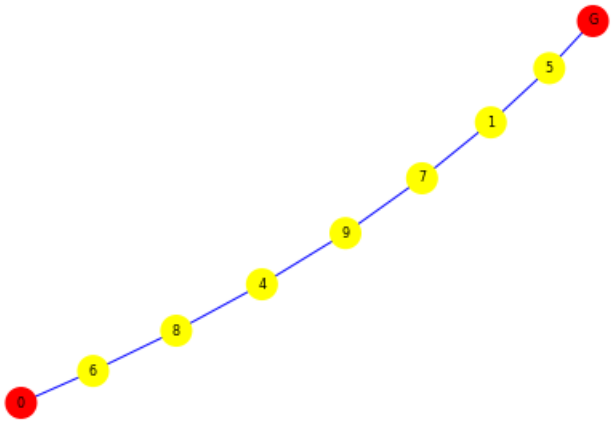
6 Picture of blockchain trees and longest chain *Stubborn Mining*

6.1 Hashing Power .25

6.1.1 Blockchain Tree

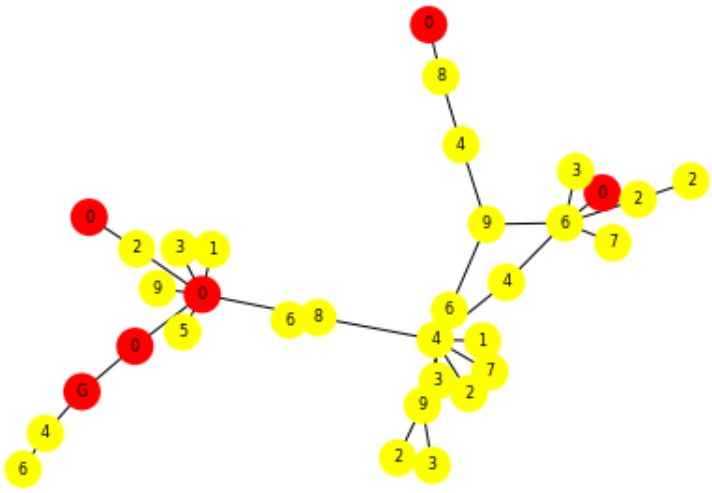


6.1.2 Longest Chain

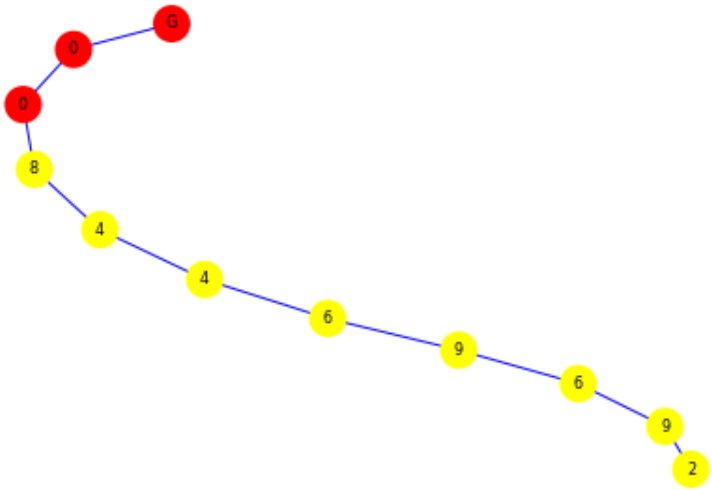


6.2 Hashing Power .50

6.2.1 Blockchain Tree

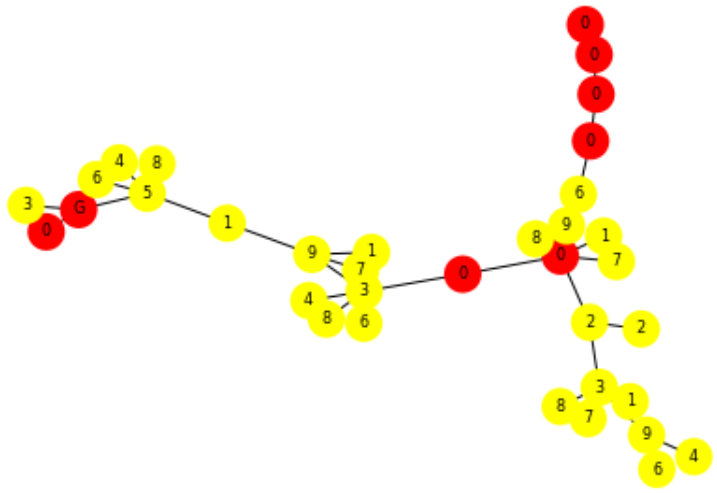


6.2.2 Longest Chain

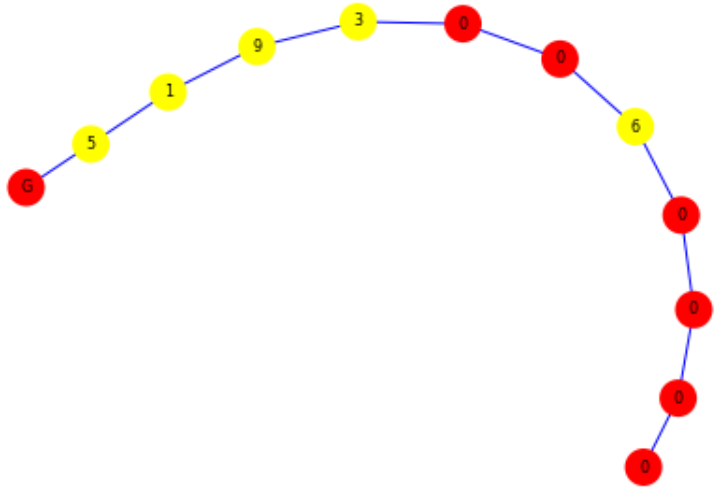


6.3 Hashing Power .75

6.3.1 Blockchain Tree



6.3.2 Longest Chain



7 Bibliography

References

[1] https://github.com/dvf/blockchain/find/master

[2] https://jis-eurasipjournals.springeropen.com/track/pdf/10.1186/s13635-019-0085-3.pdf

[3] https://medium.com/@amannagpal4/how-to-create-your-own-decentralized-file-sharing-service-using-python-2e00005bdc4a

[4] https://pypi.org/project/pyp2p/

[5] https://www.youtube.com/watch?v=b81Ib_oYbFk&list=PLBOh8f9FoHHhNmKlVW8TYKnNoCCf8srPh

[6] https://github.com/dufferzafar/crypto-simulation/blob/master/Problem%20Statement.pdf

[7] https://github.com/macsnoeren/python-p2p-network

[8] https://people.orie.cornell.edu/mru8/orie3120/lec/lec10.pdf

[9] http://cs.baylor.edu/~maurer/aida/desauto/chapter3.pdf

[10] https://www.cs.cmu.edu/~music/cmsip/readings/intro-discrete-event-sim.html

[11] https://arxiv.org/abs/1311.0243

[12] https://ieeexplore.ieee.org/abstract/document/7467362