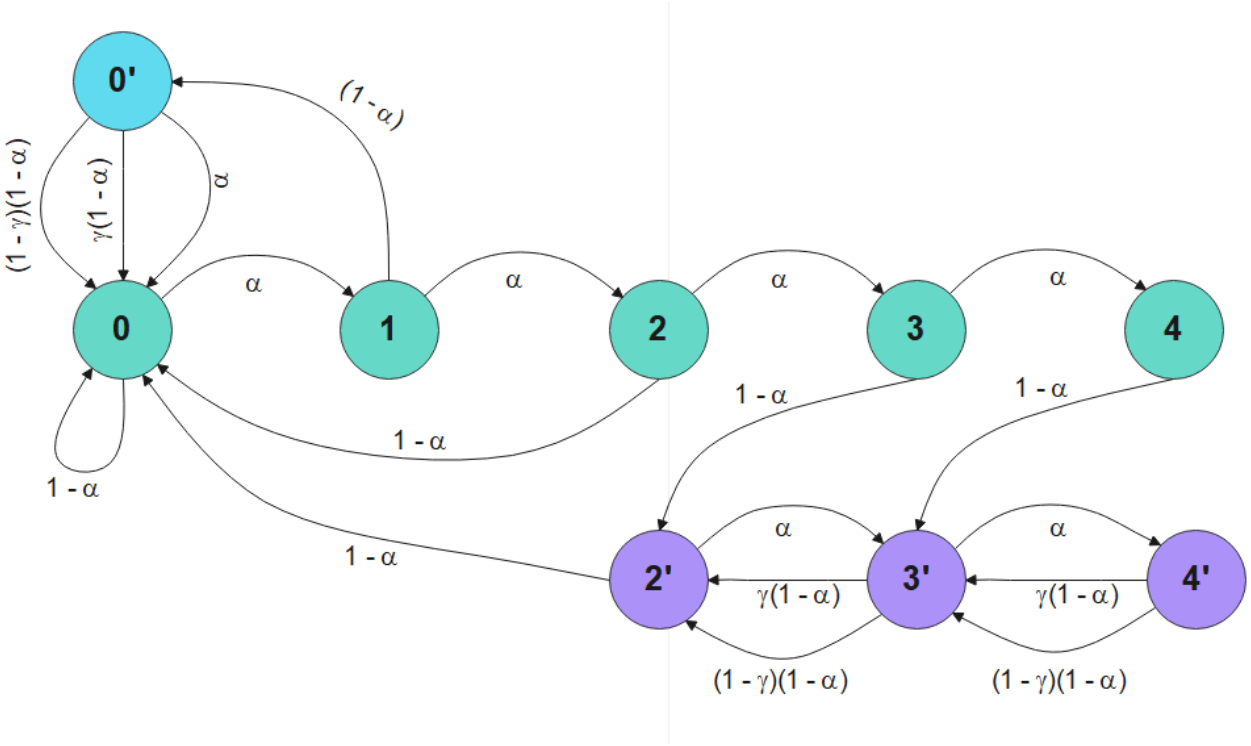
Introduction to Blockchain, Cryptocurrencies and Smart Contracts

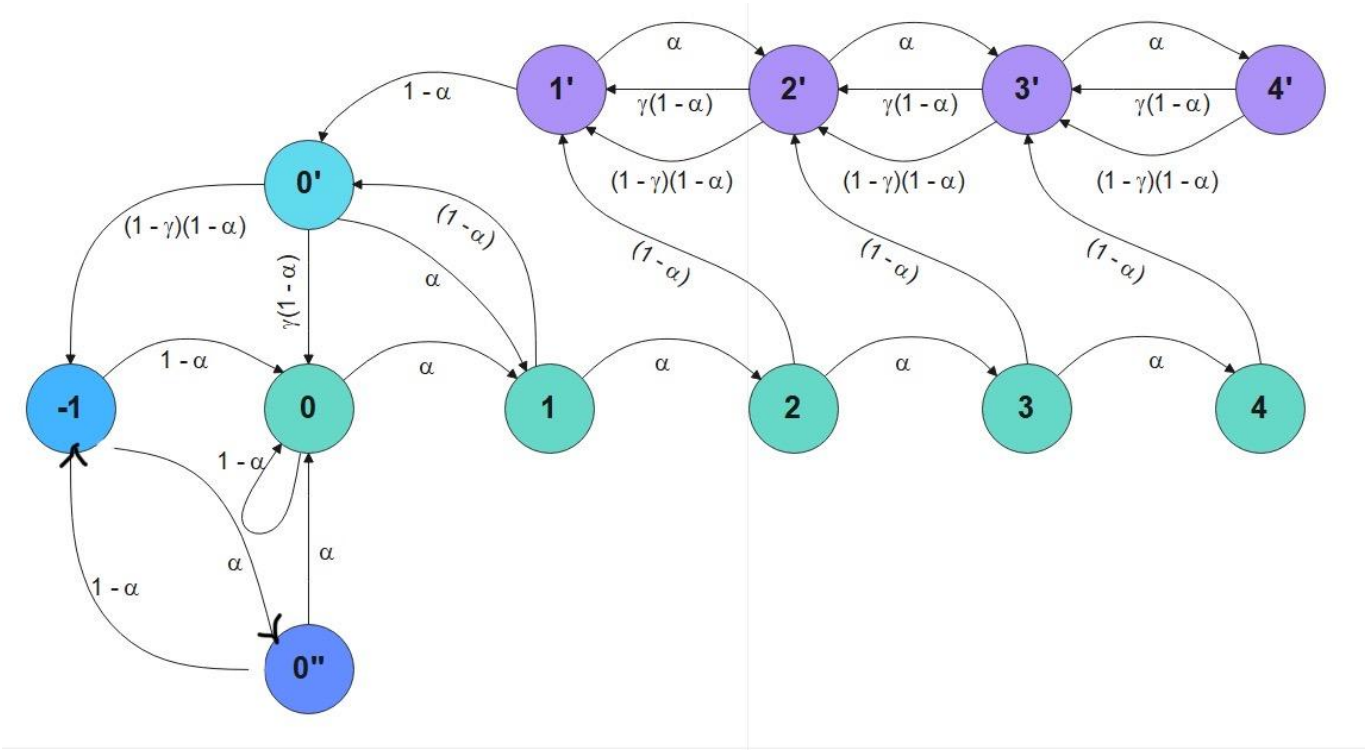
(CS 765)

Assignment 2

Rhushabh Gedam - 180050085
Utkarsh Agarwal - 180050115
Gagan Jain - 180100043
Kaushik Sen - 203044008



Markov Chain: Selfish Mining



Markov Chain: Stubborn Mining

Insights and Critique

The experimental datatable by varying parameters ($Adversary\ mining\ power$, $\zeta = 0.25,\ 0.5,\ 0.75$) and their corresponding MPU_adv and MPU_overall are as follows:

SELFISH								STUBBORN						
Seed	Adv Gamma	Adv Power	Eff fraction	MPU_Adv	MPU_overall	blockchain length		Seed	Adv Gamma	Adv Power	Eff fraction	MPU_Adv	MPU_overall	blockchain length
0	0.25	0.3	0.227	0.555	0.759	66		0	0.25	0.3	0.1774	0.2683	0.5688	62
0	0.5	0.3	0.206	0.583	0.791	68		0	0.5	0.3	0.4426	0.675	0.61	61
0	0.75	0.3	0.358	0.76	0.716	53		0	0.75	0.3	0.5094	0.6279	0.552	53
20	0.25	0.3	0.2727	0.75	0.786	66		20	0.25	0.3	0.1034	0.1538	0.6042	58
20	0.5	0.3	0.19	0.57	0.775	62		20	0.5	0.3	0.1481	0.2353	0.6207	54
20	0.75	0.3	0.264	0.864	0.828	72		20	0.75	0.3	0.25	0.5172	0.6818	60
40	0.25	0.3	0.2154	0.5385	0.7386	65		40	0.25	0.3	0.44	0.714	0.65	67

40	0.5	0.3	0.3382	0.8846	0.8	68		40	0.5	0.3	0.228	0.351	0.606	57
40	0.75	0.3	0.3889	0.8235	0.7423	72		40	0.75	0.3	0.271	0.3636	0.584	59
60	0.25	0.3	0.333	0.75	0.783	54		60	0.25	0.3	0.286	0.516	0.644	56
60	0.5	0.3	0.4	0.889	0.723	60		60	0.5	0.3	0.261	0.45	0.645	69
60	0.75	0.3	0.28	0.75	0.762	64		60	0.75	0.3	0.298	0.567	0.633	57
SELFISH								STUBBORN						
Seed	Adv Gamma	Adv Power	Eff fraction	MPU_Adv	MPU_overall	blockchain length		Seed	Adv Gamma	Adv Power	Eff fraction	MPU_Adv	MPU_overall	blockchain length
0	0.5	0.1	0.06	0.5	0.902	83		0	0.5	0.1	0.9259	0.9803	0.5869	54
0	0.5	0.3	0.206	0.583	0.791	68		0	0.5	0.3	0.4426	0.675	0.61	61
0	0.5	0.5	0.89	0.894	0.534	47		0	0.5	0.5	0.9273	0.9623	0.6044	55
0	0.5	0.7	1	0.673	0.7647			0	0.5	0.7	0.9574	1	0.5341	47

Selfish mining

It is expected and experimentally proven that MPU_adv > MPU_overall for higher values of ζ

Effective fraction of Adversary's blocks in the main chain (Eff.)

As the mining power of the adversary increases, his fraction of blocks in the main chain (Eff.) increases. More mining power implies the adversary is able to elongate his chain at a faster pace without transitioning to state=0' and take a lead of more than 1 with high probability.
This fraction is seemingly more than his mining power which proves the effectiveness of the attack.

As ζincreases, on average Eff. increases. As more honest peers are directly connected to the adversary, this attracts more honest miners to his chain and reduces the chances of being overtaken by the public chain completely. This ensures that even if he loses his private chain in state 0', he still manages to put some of his blocks into the accepted chain.

MPU_adv

As the mining power of the adversary increases, MPU_adv increases.

As ζincreases, MPU_adv increases.

MPU_overall

As mining power increases, MPU_overall increases.
As ζincreases, MPU_overall fluctuates.
This is evident as more branching is visible when the public and private blocks are in parallel. This diverts the honest mining power to do useless work and buys adversary time to further elongate his private chain.

Stubborn mining

Effective fraction of Adversary's blocks in the main chain (Eff.)

As the mining power of the adversary increases, his fraction of blocks in the main chain (Eff.) increases.

As ζincreases, on average Eff. increases.

MPU_adv

As the mining power of the adversary increases, MPU_adv increases.

As ζincreases, MPU_adv increases.

MPU_overall

As mining power increases, MPU_overall increases.

As ζincreases, more branching is visible when the public and private blocks are in parallel. This decreases the MPU_overall.