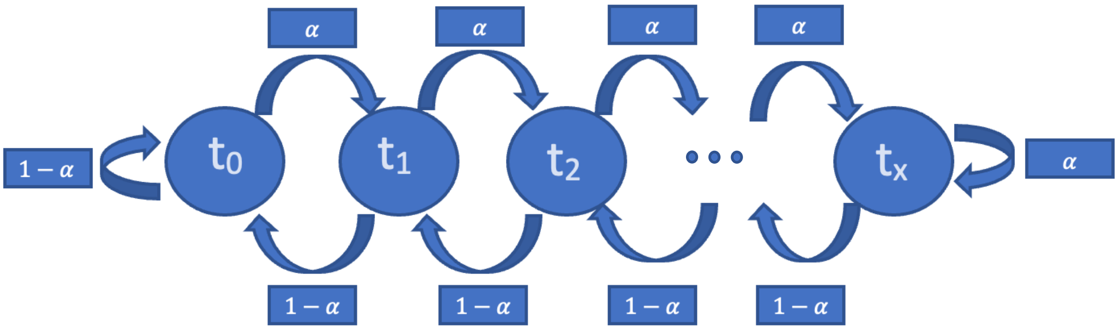
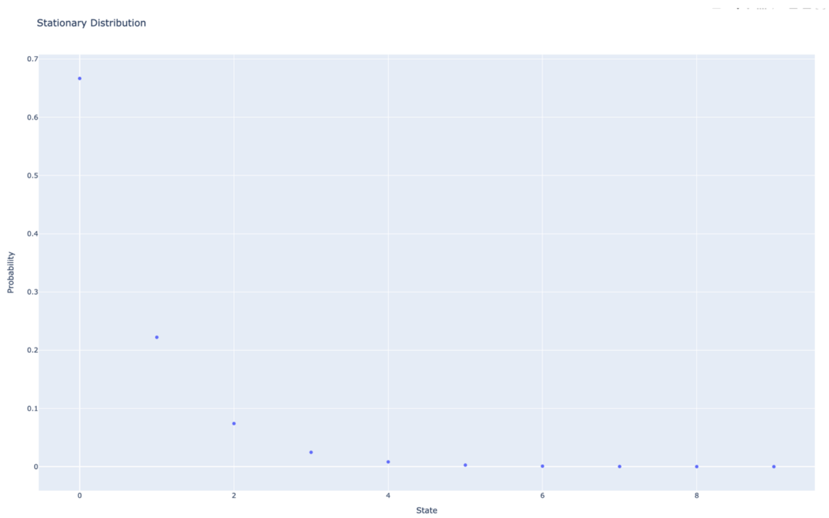
1) Let's formally describe the pre-mining attempts as a random walk. Let $x \in \mathbb{N}$:



$$\begin{aligned}
&\textit{states of the system} = \{t_0, t_1, t_2, \dots, t_x\} \\
&\mathbb{P}(t_i \to t_{i+1}) = \alpha \qquad \textit{if } i > 0 \\
&\mathbb{P}(t_{i+1} \to t_i) = 1-\alpha \quad \textit{if } i < x \\
&\mathbb{P}(t_i \to t_i) = 1-\alpha \qquad \textit{if } i = 0 \\
&\mathbb{P}(t_i \to t_i) = \alpha \qquad\quad \textit{if } i = x
\end{aligned}$$

2) The state space is infinite, so let's assume that the attacker never acquires more than a 30 block advantage; if the attacker has such an advantage and mines an extra block, that block is discarded. The first 10 probabilities of the result for an attacker that has 25% of the hash-rate. We have picked and initial distribution of p with an equal probability for every 30 states. These are the results after 1,000 iterations:

Probability of finishing on state 0: **0.66666666666666973828**
Probability of finishing on state 1: **0.22222222222222326460**
Probability of finishing on state 2: **0.07407407407407441691**
Probability of finishing on state 3: **0.02469135802469147462**
Probability of finishing on state 4: **0.00823045267489715994**
Probability of finishing on state 5: **0.00274348422496571926**
Probability of finishing on state 6: **0.00091449474165523968**
Probability of finishing on state 7: **0.00030483158055174663**
Probability of finishing on state 8: **0.00010161052685058220**
Probability of finishing on state 9: **0.00003387017561686073**



3) Prove that the following expression is the stationary distribution $p_n = C * \left(\frac{\alpha}{1-\alpha}\right)^n$

Question 3 :

$\beta = 1-\alpha \qquad T' = \begin{bmatrix} \beta & \beta & \cdots & & 0 \\ \alpha & 0 & \ddots & & \\ & \ddots & \ddots & \ddots & \\ & & \ddots & 0 & \beta \\ 0 & & & \alpha & \alpha \end{bmatrix}$

Let $n \in \mathbb{N}$ $\quad T'p_n = \begin{pmatrix} \beta & \beta & \cdots & & 0 \\ \alpha & 0 & \ddots & & \\ & \ddots & \ddots & \ddots & \\ & & \ddots & 0 & \beta \\ 0 & & & \alpha & \alpha \end{pmatrix} \cdot \begin{pmatrix} 1 \\ \alpha/\beta \\ \vdots \\ (\alpha/\beta)^n \end{pmatrix}$

N.t $(T')_{ij} = \begin{cases} \beta & i=1 \; j=1 \\ \beta & i+1=j \\ \alpha & i=j+1 \\ \alpha & i=n+1 \; j=n+1 \\ 0 & \end{cases}$

$(p_n)_i = \left(\frac{\alpha}{\beta}\right)^{i-1}$

We know from lecture that $T' \cdot p^* = p^*$. This means p^* is an eigenvector of T' with eigenvalue 1. Let's prove p_n is an eigenvector of T' $\Leftrightarrow$ $T' \cdot p_n = p_n$

$(T'_n)_{ij}(p_n)_j = \begin{cases} \beta(1+\frac{\alpha}{\beta}) & i=1 \rightarrow \alpha+\beta \checkmark \\ \alpha(\alpha/\beta)^{i-2} + \beta(\alpha/\beta)^i & \text{else } (*) \\ \alpha(\alpha/\beta)^{n-1}(1+\alpha/\beta) & i=n+1 \; (*) \end{cases}$

(*)

$\alpha \cdot (\alpha/\beta)^{i-2} + \beta(\alpha/\beta)^i \overset{?}{=} (\alpha/\beta)^{i-1}$

$\alpha \cdot (\alpha/\beta)^{i-2} + \beta(\alpha/\beta)^i = \alpha \cdot \left(\alpha/_{1-\alpha}\right)^{i-2} + (1-\alpha)\cdot\left(\frac{\alpha}{1-\alpha}\right)^i =$

$= \frac{\alpha^{i-1}}{(1-\alpha)^{i-2}} + \frac{\alpha^i}{(1-\alpha)^{i-1}} = \frac{(1-\cancel{\alpha})\cdot\alpha^{i-1}}{(1-\alpha)^{i-1}} + \cancel{\alpha} = \frac{\alpha^{i-1}}{(1-\alpha)^{i-1}}$

$= (\alpha/\beta)^{i-1} \checkmark$

(*)

$\alpha(\alpha/\beta)(1+\alpha/\beta) \overset{?}{=} (\alpha/\beta)^1$

$\alpha(\alpha/\beta)(1+\alpha/\beta) = \frac{\alpha^n}{(1-\alpha)^{n-1}} + \frac{\alpha^{n+1}}{(1-\alpha)^n} =$

$= \frac{(1-\alpha)\alpha^n + \cancel{\alpha^{n+1}}}{(1-\alpha)^n} =$

$= \alpha^n/(1-\alpha)^n \checkmark$

Notice that, we've proved that p_n is an eigenvector of T' for eigenvalue 1. Therefore, p_n normalized is the stationary distribution.

To find C, we need to make the following assumption $\alpha < 1/2$

$\frac{1}{C} = \sum_{i=0}^{\infty} (\alpha/_{1-\alpha})^i = \frac{1}{1-\frac{\alpha}{1-\alpha}} = \frac{1-\alpha}{1-2\alpha} \Rightarrow \boxed{C = \frac{1-2\alpha}{1-\alpha}}$

All in all, $\boxed{p_n = \frac{1-2\alpha}{1-\alpha}\left(\alpha/_{1-\alpha}\right)^n}$

4) Let's show that the analytical result matches the stationary distribution you computed for an attacker with 25% of the compute power.

To show that the analytical result matches the stationary distribution computed for an attacker with 25% of the compute power we have done the following:
We have picked an initial distribution of $p_0 = [1, 0\ldots0]$ and multiplied the matrix obtained at the i'th iteration. We have plotted the vector obtained for each iteration in which every index of the vector represents the probability to appear at that state on that specific iteration. We've calculated for each iteration the difference of the vector and the stationary distribution calculated on question 3 using the formula. We can appreciate from the graph a convergence to 0 for all states. Notice that, no matter which initial distribution is chosen, convergence will always be satisfied.