Final Report

D1094012 電子博一 梁峻瑋

論文：
IEEE ICC 2021 Best paper——
Analysis of Selfish Miner Behavior in the Bitcoin Network
Motlagh, Saeideh G., Jelena Mišić, and Vojislav B. Mišić. "Analysis of Selfish Miner Behavior in the Bitcoin Network." *ICC 2021-IEEE International Conference on Communications*. IEEE, 2021.

大意(Summary)：
比特幣、區塊鏈是被預期是下一個世代的網絡。其中，一種經典的攻擊手法，是礦工將挖到的區塊延遲發布、累積更多區塊，以獲取更大的利益，被稱之為「自私挖礦(Selfish mining)」。這篇論文主要在討論不同數目的自私礦工合作下，攻擊成功的機率以及系統的穩定性。

具體來說，作者使用馬可夫鏈的數學工具。作者嘗試分析隨著時間演進，自私礦工與誠實礦工各自的鏈長，以及比較自私礦工能以多少機率領先多少幅度，用來量化攻擊成功的程度、機率。事實上，攻擊成功的定義，即是維持出一條更長的鏈。

就實驗結果來看，當自私礦工人數到達總人數的一半，他們就比誠實礦工更可能拿下競賽。甚至於，他們領先4個區塊(block)的機率上看12%。在網路聯通性上，誠實礦工平均需要更多的跳數(hop)，基於自私行為的影響。這也代表，他們更缺乏競爭力來贏得比賽。

挑戰(Challenge)：
第一點，由於比特幣只有一條區塊鏈，假設自私挖礦攻擊手段被認為可行，則有可能同時出現兩個以上的攻擊團隊。然而，這篇論文只提到一個攻擊團隊的假設。

第二點，這篇論文並沒有量化自私挖礦攻擊的收益分佈，甚至是衡量收益是否為正值，或者是自私挖礦的合作能否帶來更大的獲益等等。換言之，他們還沒充分地說明自私挖礦攻擊的動機，而只是說明這樣的攻擊比防守方更有勝算一些。這確實是比較美中不足的一點。

解決方案(Solution)：
關於第一點，其實直接沿用這篇論文的模型，應該就有機會做出來。由於這篇論文，是建立在不同的自私挖礦算力之下，自私挖礦攻擊者領先區塊數的機率分佈。因此，我們只要排除不是前兩名的算力與分鏈，只用前兩名算力來套用這篇論文的模型，就可以預測出攻擊方領先區塊數的機率分佈。

換言之，除了最強攻擊者之外，其他的攻擊者均可以視為公正第三方，或者是單純浪費算力而不參與兩者的競賽。這也將造成防守方(誠實的挖礦者)被分散出更多的算力，更容易達成自私挖礦攻擊的目的。

關於第二點，初步構想是能夠描繪出一個函數，來計算自私挖礦者領先幾個區塊，就能比扮演誠實挖礦者的身份，贏得多少的收益。或許可以先從邊界條件、上下界來進行論證。